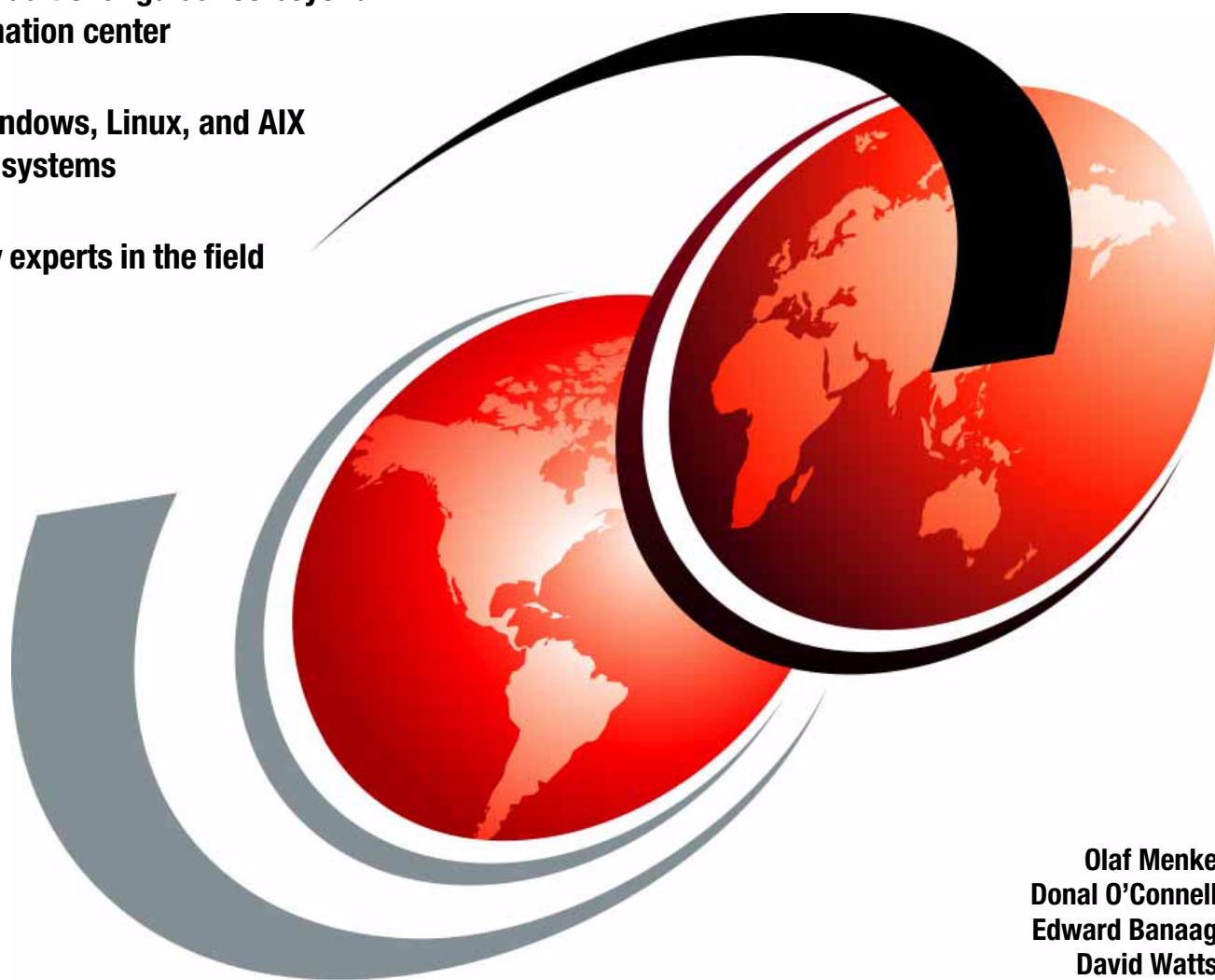


IBM Systems Director 6.3 Best Practices Installation and Configuration

Provides additional guidance beyond
the information center

Covers Windows, Linux, and AIX
operating systems

Written by experts in the field



Olaf Menke
Donal O'Connell
Edward Banaag
David Watts



International Technical Support Organization

**IBM Systems Director 6.3 Best Practices: Installation
and Configuration**

April 2013

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

First Edition (April 2013)

This edition applies to Version 6.3.2 of IBM Systems Director.

© Copyright International Business Machines Corporation 2013. All rights reserved.

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

Contents

Notices	vii
Trademarks	viii
Preface	ix
The team who wrote this paper	ix
Now you can become a published author, too!	x
Comments welcome	x
Stay connected to IBM Redbooks	xi
Chapter 1. Installation	1
1.1 Agent selection	2
1.2 IBM Systems Workload Estimator	2
1.3 System resources	7
1.4 Before you begin	8
1.5 Installing on an x86 platform	12
1.5.1 Supported operating systems	12
1.5.2 Installation on Linux on x86 systems	14
1.5.3 Installation on Windows	20
1.5.4 Post Installation Validation (PIV) tool	28
1.5.5 Starting Systems Director	31
1.6 Installing Systems Director on an AIX platform	33
1.6.1 Downloading the software	33
1.6.2 Prerequisites	34
1.6.3 Installation	36
1.6.4 DB2 settings	38
1.6.5 Initial login	41
1.6.6 Installing the Systems Director license	43
1.7 Installing on a Linux on Power platform	44
1.7.1 Downloading the software	44
1.7.2 Prerequisites	44
1.7.3 Installing the Systems Director server	47
Chapter 2. Fundamentals	51
2.1 Discovery	52
2.1.1 Discovery profiles	54
2.1.2 BladeCenter discovery	56
2.2 Endpoint management	59
2.3 Firewall ports	59
2.4 Inventory	64
2.4.1 Inventory data and collection profiles	64
2.4.2 Collecting inventory	71
2.4.3 Viewing inventory	75
2.4.4 Exporting inventory	78
2.5 Updates	82
2.5.1 Prerequisites	83
2.5.2 What can be updated	83
2.5.3 Settings for Update Manager	85
2.5.4 Update Manager with Internet connection	89
2.5.5 Update Manager with no Internet connection	91

2.5.6	Compliance check	93
2.5.7	Update process	100
2.5.8	Updating systems that run AIX and Linux	111
2.5.9	Updating the Systems Director server	113
2.5.10	Command-line tools	116
Chapter 3. Advanced functions		119
3.1	Hardware Management Console and AIX Launch-in-Context	120
3.2	Light path diagnostics	134
3.2.1	LED status in the scoreboard	134
3.2.2	LED status in the Resource Explorer	136
3.2.3	LED Status from the menu of a system	138
3.2.4	SMCLI command-line interface	138
3.3	Hardware logs	139
3.4	Service and Support Manager	143
3.4.1	Connectivity to IBM	145
3.4.2	Enabling systems for service and support	146
3.4.3	Serviceable event processing	148
3.4.4	Managing support files	148
3.5	Event logs	150
3.5.1	Settings	151
3.5.2	Launching the event log	152
3.5.3	Viewing the event log	153
3.5.4	Using event filters	155
3.5.5	Creating a filter by using an event from the event log	156
3.5.6	Command-line tools	158
3.6	Automation Manager	160
3.6.1	Creating an event automation plan	161
3.6.2	Creating an event filter	172
3.6.3	Creating an event action	182
3.6.4	Using the CLI for event automation plans	188
3.7	Security	190
3.7.1	Users and groups for authentication	191
3.7.2	Authorizing users	193
3.7.3	Access managed systems	201
3.7.4	Credentials	204
3.7.5	Lightweight Directory Access Protocol	204
3.7.6	Using command-line tools for security	214
3.7.7	Error logs and troubleshooting	216
Chapter 4. Backup		219
4.1	Backup Q&A	220
4.2	Backup and recovery	220
4.2.1	Systems Director backup	220
4.2.2	Systems Director restore	223
4.2.3	Systems Director reset	224
4.3	Migration	225
4.3.1	Exporting systems and settings	225
4.3.2	Exporting settings	226
4.3.3	Importing systems and settings	228
Chapter 5. Additional information and education		233
5.1	Information center	234
5.2	Social media and support	234

5.2.1 Forum	234
5.2.2 Wiki	235
5.2.3 YouTube channel	236
5.2.4 Facebook page	236
5.2.5 My Notifications email announcements.....	237
5.3 Education and training	237
5.3.1 Integrated education modules in Systems Director.....	238
5.3.2 Education courses	241
5.4 Downloads	241
5.5 Other useful links	242
Abbreviations and acronyms	245
Related publications	247
IBM Redbooks	247
Online resources	247

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 grant 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

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

Trademarks

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

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

AIX®	IBM®	Redbooks (logo)  ®
BladeCenter®	Lotus®	System i®
DB2®	Power Systems™	System p®
Domino®	POWER6®	System x®
Electronic Service Agent™	POWER®	Tivoli®
i5/OS™	PureFlex™	
IBM Flex System™	Redbooks®	

The following terms are trademarks of other companies:

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

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

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Preface

IBM® Systems Director is a platform management foundation that streamlines the way that physical and virtual systems are managed. Using industry standards, IBM Systems Director supports multiple operating systems and virtualization technologies.

This paper provides guidance and preferred practices about how to install and configure IBM Systems Director Version 6.3. Also, installation guidance, fundamental topics, such as discovery and inventory, and more advanced topics, such as troubleshooting and automation, are covered.

This paper is meant to be a partner to the comprehensive documentation in the IBM Systems Director Information Center. This paper is aimed at IT specialists who are planning to install and configure Systems Director on Microsoft Windows, Linux, or IBM AIX®.

The team who wrote this paper

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



David Watts is a Consulting IT Specialist at IBM in Raleigh, North Carolina, in the US. He manages residencies and produces IBM Redbooks® publications about hardware and software topics that relate to IBM Flex System™, IBM System x®, and IBM BladeCenter® servers and associated client platforms. He has authored over 300 books and papers. He holds a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM in both the United States and Australia since 1989. David is an IBM Certified IT Specialist and a member of the IT Specialist Certification Review Board.



Olaf Menke is a consultant and subject matter expert for systems management. He has worked in the IBM Technical Sales Support (TSS) Software Service in IBM Germany for the past two years. Prior to this position, he was a Systems Engineer and IBM System x and BladeCenter specialist in the System x Pre-Sales team in Germany. He has over 16 years of experience in support of computer systems and software. He holds a degree in Information Technology from the Technische Universitaet in Dresden. His areas of expertise include System x, BladeCenter, IBM PureFlex™, Systems Director, and management hardware. He is an IBM Certified Specialist for PureFlex and IBM Certified Expert for IBM System x and BladeCenter.



Donal O'Connell is a Lab Services Consultant for IBM Systems and Technology Group, located in Dublin, Ireland. In this role, he implements emerging technologies on behalf of IBM clients through services-based offerings. He has expertise in IBM Power Systems™, PureFlex System, and systems management for AIX using Systems Director and IBM Tivoli® Monitoring. He is a graduate of Trinity College Dublin.



Edward Banaag has been with IBM for 12 years and is a member of the IBM System Software Blackbelt team. Prior to his current role, Edward was a System x Field Technical Sales Support (FTSS) specialist. He specializes in System x, BladeCenter, and PureFlex System solutions, and management tools, such as Advanced Management Module (AMM), Integrated Management Module (IMM), Chassis Management Module (CMM), and Flex System Manager. He also has expertise across various x86 technologies, including server operating systems, virtualization technologies, and networking technologies.

Thanks to the extended residency team for their contributions to this project through developing the outline and reviewing the written material:

- ▶ Kevin Carter
- ▶ Brandon Harrell
- ▶ Daniel Weiss
- ▶ Josh Dembling
- ▶ Craig Elliott

Now you can become a published author, too!

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

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

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:

<http://www.facebook.com/IBMRedbooks>

- ▶ Follow us on Twitter:

<http://twitter.com/ibmredbooks>

- ▶ Look for us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- ▶ Stay current on recent Redbooks publications with RSS Feeds:

<http://www.redbooks.ibm.com/rss.html>



Installation

The installation of IBM Systems Director 6.3 server with recommendations is discussed. Because this paper is a preferred practices guide, we did not list all permutations that relate to Systems Director. Obtain this information by reading the *IBM Systems Director Planning Guide*, which is available from this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_planning.html

The following topics are covered:

- ▶ 1.1, “Agent selection” on page 2
- ▶ 1.2, “IBM Systems Workload Estimator” on page 2
- ▶ 1.3, “System resources” on page 7
- ▶ 1.4, “Before you begin” on page 8
- ▶ 1.5, “Installing on an x86 platform” on page 12
- ▶ 1.6, “Installing Systems Director on an AIX platform” on page 33
- ▶ 1.7, “Installing on a Linux on Power platform” on page 44

1.1 Agent selection

Systems Director performance and scalability are intrinsically linked to the allocated resources, number of discovered systems, and associated management type. Systems Director is a platform management tool that gives a single view to managing a heterogeneous environment across multiple operating systems and platforms.

The Systems Director user interface provides a uniform view for managing discovered systems by determining where those systems are in the managed environment. Systems come with preset functionality from Systems Director. Additional functionality is available, depending on the agent type that is installed on each endpoint that each operating system is running.

The IBM Systems Director Information Center helps you choose the level of agent capabilities to deploy on managed systems:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_t_agent_tiers.html

1.2 IBM Systems Workload Estimator

IBM Systems Workload Estimator for Systems Director 6.3 is a web-based tool that can size hardware for systems that run the Systems Director server. The tool is presented in a Q&A format and requests user input.

Launch the IBM Systems Workload Estimator for Systems Director 6.3 from this URL:

<http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Fwle.html>

You might be asked to enter user demographic information as shown in Figure 1-1.

The screenshot shows the 'User Demographic Information' window of the IBM Systems Workload Estimator. The page has a dark blue header with the IBM logo and a search bar. Below the header is a navigation menu with links for Home, Business solutions, IT services, Products, Support & downloads, and My IBM. The main content area is titled 'User Demographic Information' and contains a form with the following fields:

- Country/Region:** A dropdown menu with the text 'Please Choose One'.
- Language:** A dropdown menu with the text 'English'.
- Number Formatting:** A dropdown menu with the text 'United States Style (1,234,567.89)'.
- User type:** A list of radio buttons with the following options:
 - I am an end-user or customer
 - I am an Independent Software Vendor (ISV)
 - I am a hardware reseller or Business Partner
 - I am an IBM sales/field/Techline employee
 - I am a general IBM employee

Below the form is a blue 'Continue' button with a right-pointing arrow. At the bottom of the page, there is a footer with the text 'IBM Systems Workload Estimator v2012.3 23-Oct-2012 www-912' and a 'Feedback' link.

Figure 1-1 User Demographic Information window

If you are not asked for demographic information, the window that is shown in Figure 1-2 opens. The platform, database, and plug-in type are listed in Figure 1-2.

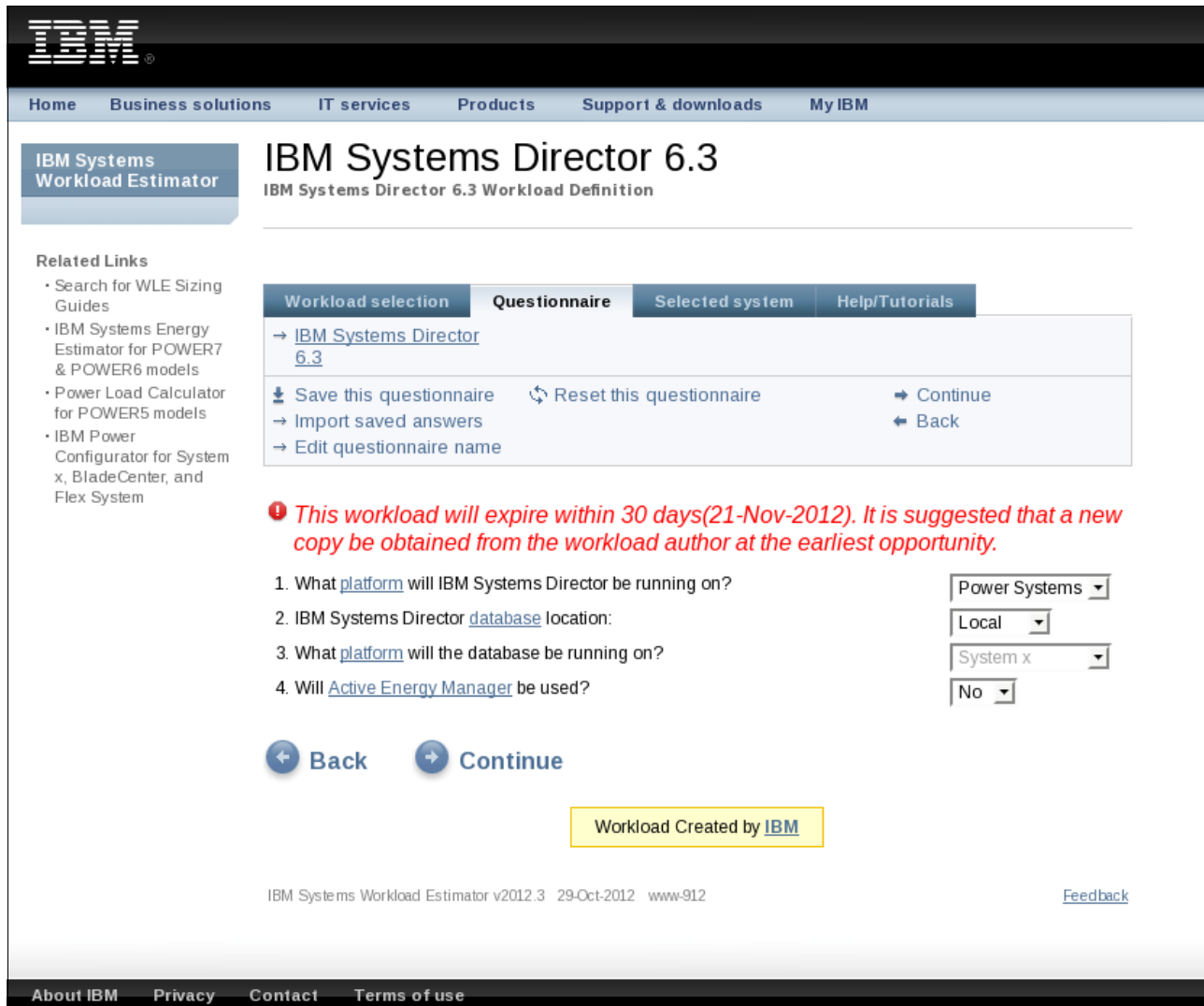


Figure 1-2 Platform choice

In Figure 1-2, the Active Energy Manager plug-in is listed due to the additional I/O, network traffic, and processor utilization activity that result from collecting data from your energy consumption.

Figure 1-3 requests information about the operating system on which you chose to install the Systems Director server, the estimated console activity that is projected with the managed environment, and the number of concurrent users.

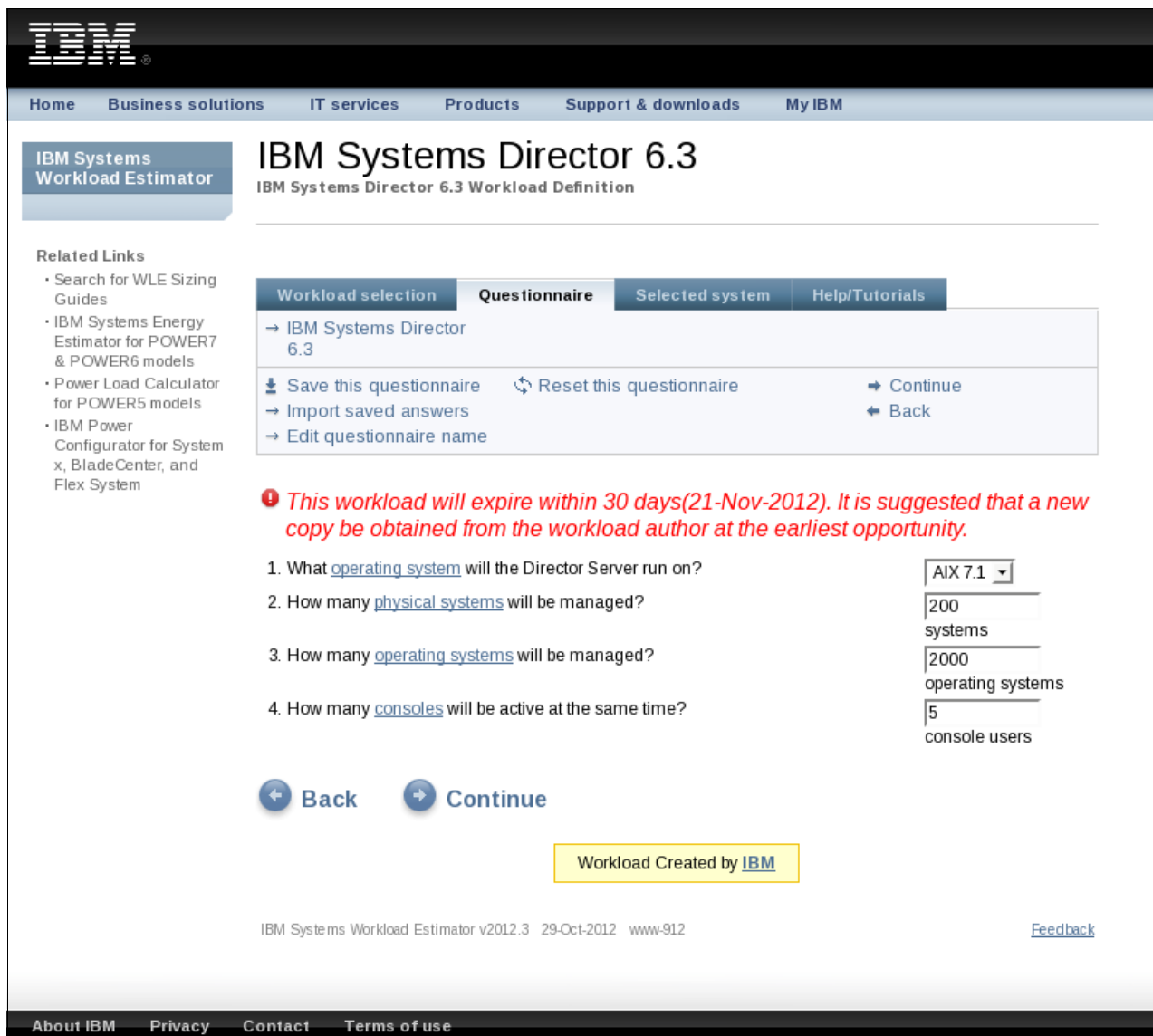


Figure 1-3 OS and usage

The estimator provides guidance for the number of required disk drives for external storage (Figure 1-4).

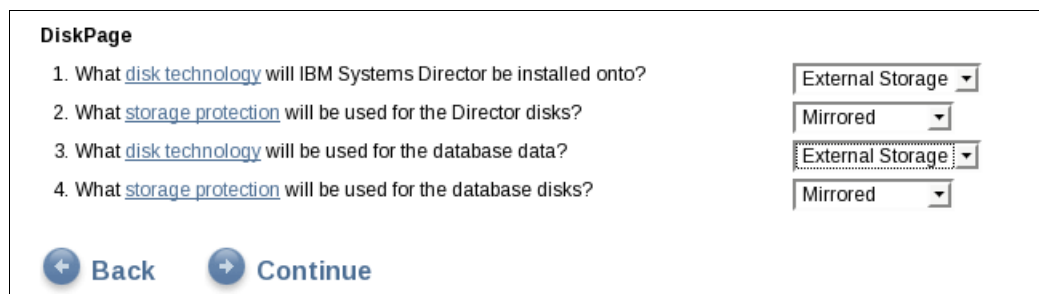


Figure 1-4 Storage

On the completion of all the fields, the Workload Estimator provides two *estimated* outputs. One estimate is for an immediate solution, and the other estimate is for a growth solution (Figure 1-5).

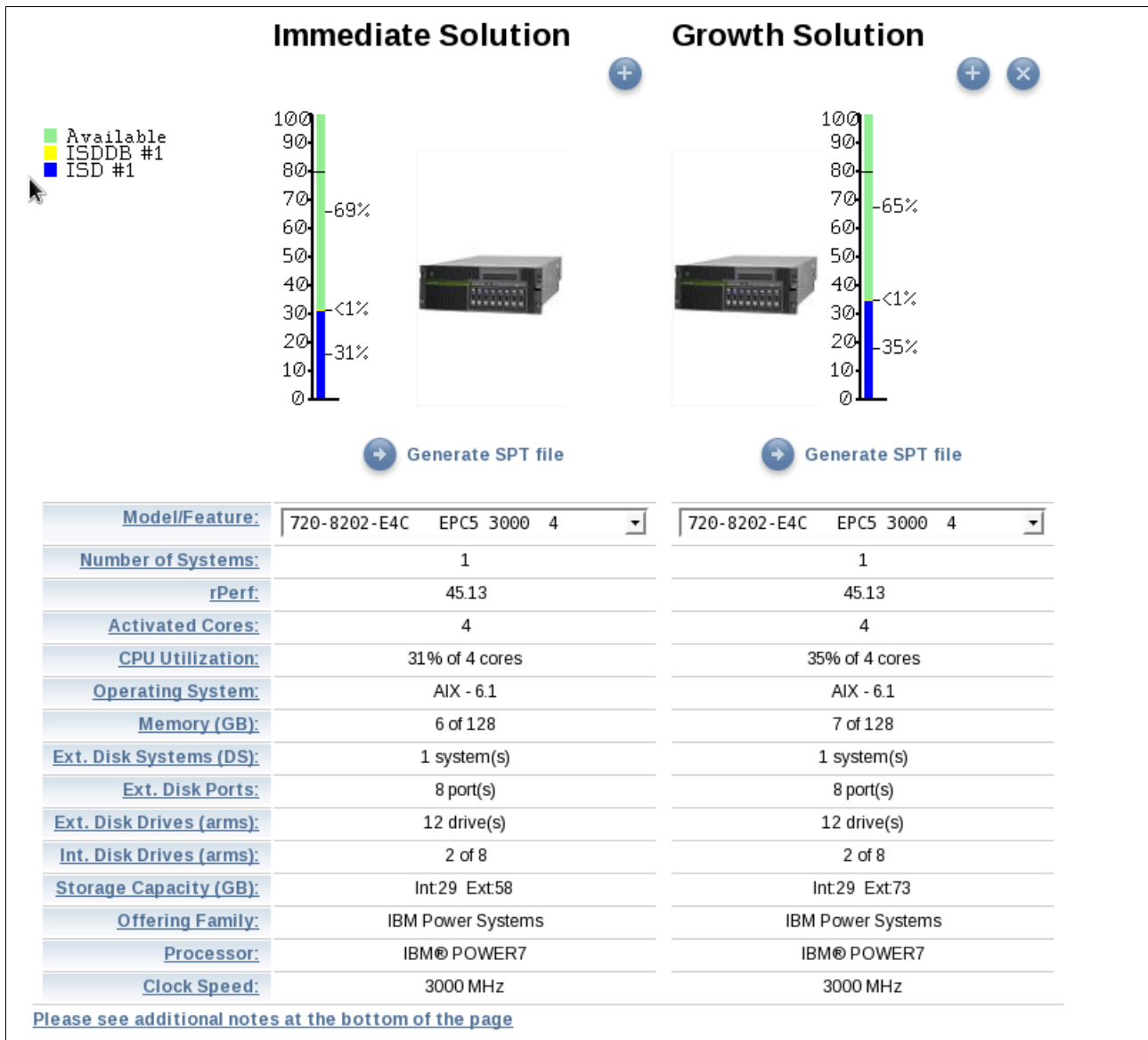


Figure 1-5 Workload Estimator proposed solution

You can further modify the configuration by reviewing the selected system and by using the modify section as shown in Figure 1-6.

Workload selection	Questionnaire	Workload definition	Selected system	Help
Save all workloads	→ Modify topology		← Back	
Generate PDF	→ Modify/visualize system		→ Retired sizing	
Printable version	→ Modify external storage		→ Show possible systems	
→ Edit estimation info	→ Modify disk groups		↻ Recalculate	
→ Modify Opportunity #	→ Modify growth factors		→ Export to SCON	
→ User options	→ Modify horizontal scaling		↻ Resize to User Options	
	→ Modify VIOS			
	→ Modify Chassis			

Figure 1-6 Modify the Workload Estimator selection

This output does not imply that you acquire new hardware. Although, this output can be used as a guide to place a system in an environment that has available resources.

1.3 System resources

Table 1-1 is a guide for the installation of Systems Director on Power Systems. Use Table 1-1 to estimate the system resources to allocate to the logical partition (LPAR) on which the Systems Director server is installed.

Table 1-1 Systems Director hardware requirements for medium to large environments

Operating system	Processor	Memory	Disk storage
AIX/Linux	Four processors, POWER5, IBM POWER6®, or POWER7: <ul style="list-style-type: none"> ▶ Entitlement = 4 ▶ Uncapped ▶ Virtual processor = 8 ▶ Weight = default 	12 GB	30 GB
Microsoft Windows	Four processor cores (two dual-core processors or one quad-core processor)	16 GB	30 GB plus space for Update Manager files
Linux on x86	Four processor cores (two dual-core processors or one quad-core processor)	16 GB	30 GB plus space for Update Manager files
Guest OS on virtualized environment on x86	Four vCPUs	16 GB	30 GB plus space for Update Manager files
Recommendations are based on 64-bit Java virtual machine (JVM). Recommendations are based on Power 6, Intel Xeon processor numbers for x86. I/O requirements: SCSI/serial-attached SCSI (SAS) adapters and multiple 10K - 15K rpm disks. Suggested: Two processors minimum and 8-GB memory minimum. Disk storage depends on advanced managers, the used database (local/remote), and the number of systems for the Update Manager repository size. Advanced manager might require more memory (for performance).			

Table 1-1 references a medium-to-large environment.

Installation sizes are summarized in Table 1-2.

Table 1-2 Definitions for small, medium, and large installations

Configuration size	Managed systems
Small	< 500 Common Agent-managed systems
Medium	500 > Common Agent-managed systems < 1000
Large	1000 > Common Agent-managed systems < 5000

The installation media for the Systems Director server includes an integrated IBM DB2® database. Use the integrated DB2 database as the default database to simplify the installation and reduce the need for a database administrator.

The components in Figure 1-7 show points to consider when you design and implement the Systems Director server from a loading viewpoint.

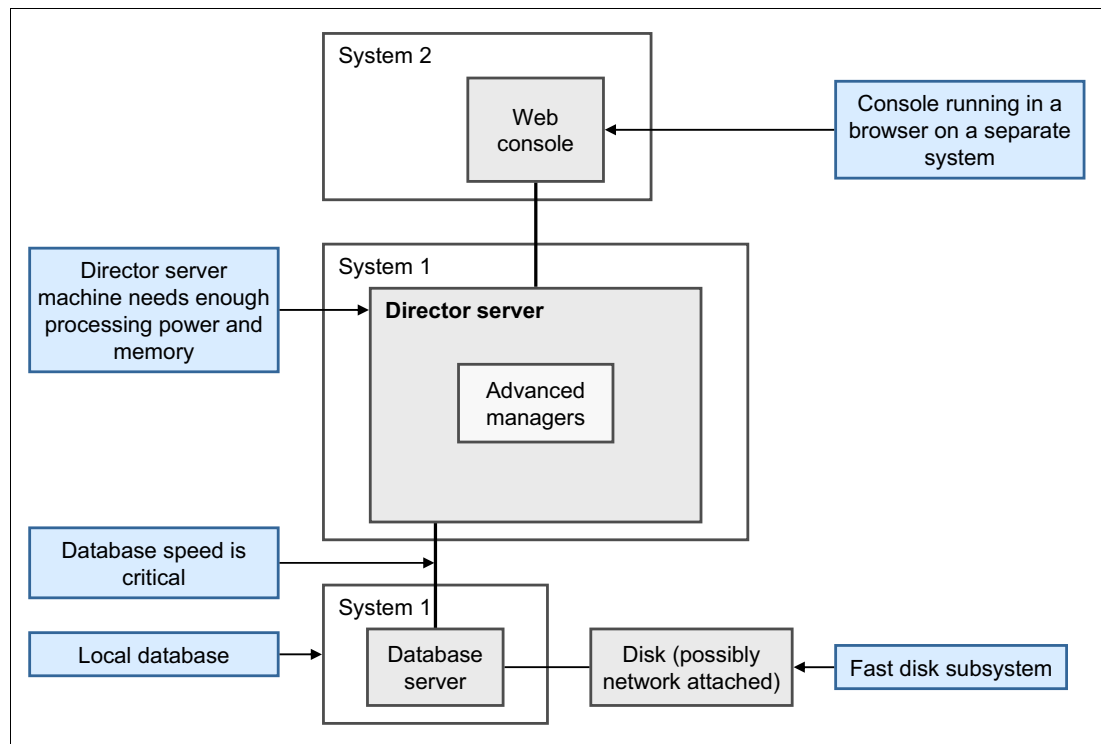


Figure 1-7 Systems Director components

1.4 Before you begin

Before the installation, review the requirements that are applicable to the operating system that you use for the installation and the current hardware environment.

Management server: Carefully plan the hardware and virtualization environment to be managed by the management server.

Hardware requirements are listed in the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.plan.helps.doc/fqm0_r_hardware_requirements.html

The supported operating systems are listed in the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_supported_operating_systems.html

Security features and considerations are documented in the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_c_security.html

The primary tasks are listed:

- ▶ Install the Systems Director server.
- ▶ Configure Agent Manager.
- ▶ Start the Systems Director server.
- ▶ Update the Systems Director server.

File system requirements that are needed for the installation are documented at this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_hardware_requirements_servers_running_aix.html

The installation of the Systems Director server is not the only step during the setup phase. Figure 1-8 on page 10 illustrates the interaction within Systems Director and the interactions among the components of the server:

- ▶ Command-line interface (CLI) interaction
- ▶ Operating system and hardware
- ▶ Network speed
- ▶ Disk subsystem
- ▶ Database activity
- ▶ Concurrent users
- ▶ Managed systems

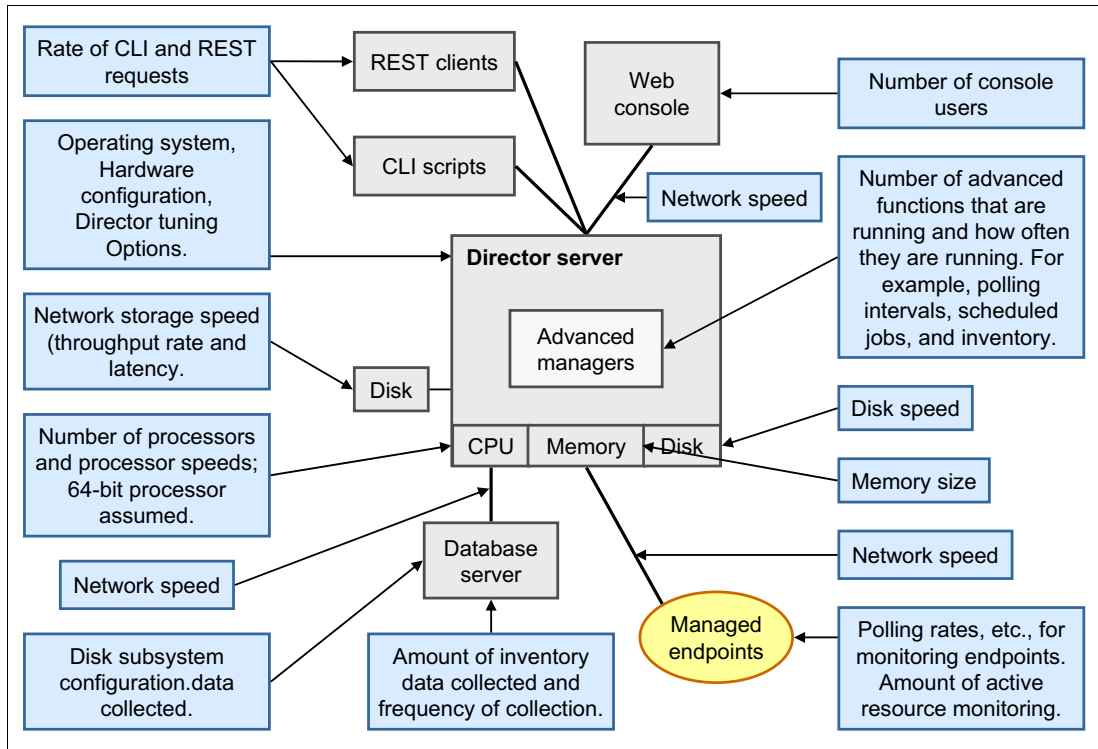


Figure 1-8 Systems Director interaction

When it comes to placement of the Systems Director server, network connectivity is critical, including DMZs and network firewalls. If firewalls are placed between the management server and the systems to be managed, changes must be made to allow for the required information flow.

A list of all TCP/IP ports that are used by Systems Director are listed at this link:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Fqm0_r_all_available_ports.html

Figure 1-9 displays a flow from the Systems Director server to a discovered Hardware Management Console (HMC) and AIX operating systems.

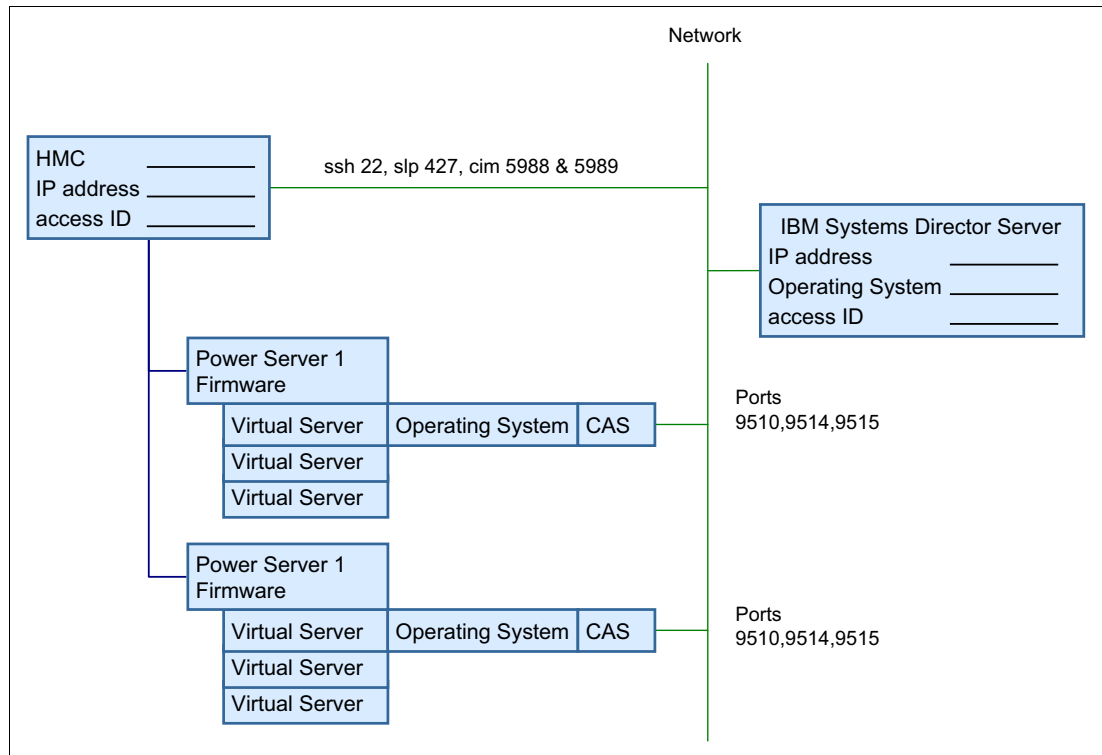


Figure 1-9 Sample connectivity for Power Systems

Before the installation of the Systems Director server, ensure that no server ports are in use by using the **netstat** and **rmssock** commands. Figure 1-10 lists examples of the **netstat** command for active ports.

```
-bash-3.2# netstat -Aan | egrep "951(0|4|5)| grep LISTEN"
f1000e00110173b8 tcp      0      0 *.9510          *.*          LISTEN
f1000e000142d3b8 tcp4    0      0 127.0.0.1.9514  *.*          LISTEN
f1000e0003b883b8 tcp4    0      0 127.0.0.1.9515  *.*          LISTEN
-bash-3.2# rmssock f1000e00110173b8 tcpcb
The socket 0xf1000e0011017008 is being held by process 23134290 (java).
-bash-3.2# ps -ef | grep 23134290
    root 23134290 35455054  0   Oct 22   -   8:51
    /var/opt/tivoli/ep/_jvm/jre/bin/java -Xmx384m -Xminf0.01 -Xmaxf0.4
    -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
    -Xbootclasspath/a:/var/opt/tivoli/ep/runtime/core/eclipse/plugins/com.ibm.rcp.base_6.2.3
    .20110824-0615/rcpbootcp.jar:/var
```

Figure 1-10 The netstat -Aan and rmssock commands

By using the **netstat** and **rmssock** commands, we can see which process is holding the port. We can take corrective action to free the port before the Systems Director server installation.

An alternate to the **netstat** and **rmssock** commands is to use the **lsof** command to list open files. Download **lsof** from this link:

<http://www-03.ibm.com/systems/power/software/aix/expansionpack/index.html>

The **netcat** command is an option for both TCP and User Datagram Protocol (UDP) to check connectivity between machines as shown in Figure 1-11.

```
-bash-3.2# netcat -zv 9.42.171.23 389
xs-2120rhelppc.itso.ral.ibm.com [9.42.171.23] 389 (ldap) open
-bash-3.2# netcat -zv 9.42.171.23 9510
xs-2120rhelppc.itso.ral.ibm.com [9.42.171.23] 9510 (?) open
-bash-3.2#
```

Figure 1-11 The netcat command

1.5 Installing on an x86 platform

The Systems Director server runs on a Windows or Linux platform on x86 systems, but only on hardware that is branded IBM (a license requirement). The Systems Director Information Center has a complete list of all supported hardware:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_hardware_compatibility.html

One way to use Systems Director on x86 is to install the Systems Director server on a virtual machine under the control of a hypervisor, such as VMware ESX or Linux Kernel-based Virtual Machine (KVM). A virtual machine offers advantages that make it a useful installation method:

- ▶ Hardware independence of certain components and drivers
- ▶ Simple extensibility of resources (memory and processor allocation)
- ▶ The ability to perform snapshots before the installations of plug-ins and advanced managers

When you use a virtual machine, we suggest that you configure four vCPUs and 16 GB or more of memory. The disk drive size depends on the number of systems and the database that is used for the Systems Director installation.

1.5.1 Supported operating systems

The Systems Director server is supported on the following operating system versions that run on IBM x86 servers:

- ▶ Linux 32-bit:
 - Red Hat Enterprise Linux Advanced Platform, version 5.0 (supports Updates 2, 3, 4, 5, 6, 7, and 8)
 - Red Hat Enterprise Linux, version 5.0 (supports Updates 1, 2, 3, 4, 5, 6, 7, and 8)
 - Red Hat Enterprise Linux Advanced Platform, version 6.0 (with or without Updates 1, 2, and 3)
 - Red Hat Enterprise Linux, version 6.0 (with or without Updates 1, 2, and 3)
 - SUSE Linux Enterprise Server 10 for x86 (supports Service Packs (SP) 2, 3, and 4)
 - SUSE Linux Enterprise Server 11 for x86 (with or without SP 1 and SP 2)
- ▶ Linux 64-bit:
 - Red Hat Enterprise Linux Advanced Platform, version 5.0, for AMD64 and EM64T (supports Updates 2, 3, 4, 5, 6, 7, and 8)

- Red Hat Enterprise Linux, version 5.0, for AMD64 and EM64T (supports Updates 2, 3, 4, 5, 6, 7, and 8)
- Red Hat Enterprise Linux Advanced Platform, version 6.0, for AMD64 and EM64T (with or without Updates 1, 2, and 3)
- Red Hat Enterprise Linux, version 6.0, for AMD64 and EM64T (with or without Updates 1, 2, and 3)
- SUSE Linux Enterprise Server 10 for AMD64 and EM64T (supports SP 2, SP 3, and SP 4)
- SUSE Linux Enterprise Server 11 for AMD64 and EM64T (with or without SP 1 and SP 2)
- ▶ Windows 32-bit:
 - Windows Server 2003, Enterprise, and Standard Editions, Release 2 (supports SP 2)
 - Windows Server 2003, Enterprise, and Standard Editions (supports SP 2)
 - Windows Server 2008, Enterprise, and Standard Editions (supports SP 1 and SP 2)
- ▶ Windows 64-bit:
 - Windows Server 2003, Enterprise, and Standard x64 Editions, Release 2 (supports SP 2)
 - Windows Server 2003, Enterprise, and Standard x64 Editions (supports SP 2)
 - Windows Server 2008, Enterprise, and Standard x64 Editions (supports SP 1 and SP 2)
 - Windows Server 2008, Enterprise, and Standard x64 Editions, Release 2 (with or without SP 1)

A detailed list of supported operating systems for the Systems Director server and agents is available at the following link:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_os_supported_by_ibm_director_631.html

You can install Systems Director on a guest OS that runs on a virtualized environment.

The supported guest operating systems are supported by both Systems Director and the hypervisor. The following conditions must be true:

- ▶ The OS platform is supported by Systems Director.
- ▶ The OS platform is supported as a guest OS by a hypervisor.
- ▶ The hypervisor is supported by Systems Director.

With these three conditions, Systems Director support of the OS platform extends to running it as a guest OS on that hypervisor. See the hypervisor product documentation for a list of supported operating systems.

The following hypervisors for the x86 environment are supported:

- ▶ VMware ESX 4.0.x and 4.1.x
- ▶ VMware ESXi 4.0.x and 4.1.x (under the control of VMware vCenter)
- ▶ VMware vSphere 5.0.x and 5.1.x (under the control of VMware vCenter)
- ▶ Linux KVM
- ▶ Windows Server 2012 and Windows Server 2008 and 2008R2, Enterprise, Standard, and Datacenter x64 Editions with Hyper-V role-enabled

Required resources: The Systems Director server is only supported on hardware that is branded IBM. Therefore, the hypervisor must run on IBM hardware to meet the license requirements.

Resources that are required for running the Systems Director server are referenced in 1.2, “IBM Systems Workload Estimator” on page 2, 1.3, “System resources” on page 7, and 1.4, “Before you begin” on page 8.

If you run firewalls in your environment, ensure that the necessary ports for the Systems Director server are open. A list of the TCP/IP ports that are used by the Systems Director server is at the following link:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Fqm0_r_ports_for_the_management_server.html

1.5.2 Installation on Linux on x86 systems

For the installation of Systems Director on Linux on x86, use the instructions in the Information Center:

https://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.install.helps.doc/fqm0_t_installing_ibm_director_server_on_linux_for_xseries.html

You can download the Systems Director server software from the following page. You need to log in with your IBM ID. Free registration is available if you do not have an ID:

<http://ibm.com/systems/software/director/downloads/mgmtservers.html>

For the installation, complete the following checks before the installation of Systems Director. These checks can be completed in any order:

- ▶ Sizing

The IBM Systems Workload Estimator for Systems Director 6.3 is a web-based tool. This tool provides hardware sizing suggestions for systems that run the Systems Director server. Launch the Workload Estimator from this URL:

<http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Fwle.html>

- ▶ Required packages for Linux on System x

Table 1-3 on page 15 lists the required packages to install Systems Director 6.3.2 on Linux.

Tip: SLES11 installs all required packages by default.

Table 1-3 Required packages for Linux on x86

Linux distribution	Management server	Common Agent	Platform Agent
RHEL	openssh libstdc++.so.5 libm.so.6 libgcc_s.so.1 libc.so.6 libdl.so.2 libpthread.so.0 unzip libaio libcrypt.so.1 libnsl.so.1 libpam.so.0 librt.so.1 bind-utils net-tools libstdc++.so.6 libuuid.so.1 libexpat.so.0	libcrypt.so.1 libc.so.6 libdl.so.2 libstdc++.so.5 libgcc_s.so.1 libm.so.6 libnsl.so.1 libpam.so.0 libpthread.so.0 librt.so.1 unzip bind-utils net-tools libstdc++.so.6 libuuid.so.1 libexpat.so.0	libstdc++.so.5 bind-utils net-tools libpam.so.0 libstdc++.so.6 libuuid.so.1 libcrypt.so.1 unzip libexpat.so.0
SLES10 SLES11	openssh libstdc++.so.5 libm.so.6 libgcc_s.so.1 libc.so.6 libdl.so.2 libpthread.so.0 unzip libaio libcrypt.so.1 libnsl.so.1 libpam.so.0 librt.so.1 bind-utils net-tools libstdc++.so.6 libuuid.so.1 libexpat.so.1	libcrypt.so.1 libc.so.6 libdl.so.2 libstdc++.so.5 libgcc_s.so.1 libm.so.6 libnsl.so.1 libpam.so.0 libpthread.so.0 librt.so.1 unzip bind-utils net-tools libstdc++.so.6 libuuid.so.1 libexpat.so.1	libstdc++.so.5 bind-utils net-tools libpam.so.0 libstdc++.so.6 libuuid.so.1 libcrypt.so.1 unzip libexpat.so.1

Installation on Linux for x86

To install the Systems Director server on Linux on x86, follow these steps:

1. Download the installation package from the IBM Systems Director Downloads website:

<http://ibm.com/systems/software/director/downloads/mgmtservers.html>

2. Extract the contents of the installation package with the following command:

```
tar -zxvf package_name
```

The *package_name* is the file name of the download packages. Alternatively, you can mount the DVD image to your system.

3. Change to the directory of the installation script. Type the following command to run the pre-installation check and press Enter:

```
../checkds/./checkds.sh
```

Reports are generated and results are displayed in the command window or the default browser. For more information, see the `/checkds/readme.txt` file.

When the result shows no errors (return code= 0) or you can explain the error message that is displayed, continue with the installation.

In our example, we got an error code/return code 34. In our example, the Systems Director server is installed on a virtual system. No baseboard management controller (BMC) or Intelligent Peripheral Management Interface (IPMI) driver is installed. In Figure 1-12 on page 17, you can see the output from the pre-installation check in the browser.

IBM Systems Director Pre-Installation Utility scans the local system to identify potential problems that could prevent IBM Systems Director from installing successfully. The utility does not scan for device driver or firmware requirements.























Scan Results	
Hardware Platform:	64 bit
Operating System:	SUSE Linux Enterprise Server 11.0 64
IBM Systems Director Type:	IBM Systems Director Server
IBM Systems Director Version:	6.3.2
Overall Report Return Code:	34
 Your system is currently failing 0 of 21 checks.	
 Your system is currently showing warnings for 1 of 21 checks.	
 ▶ Check 1: Administrator / Root Authority	
 ▶ Check 2: OS Compatibility ? Learn more	
 ▶ Check 3: Host Architecture	
 ▶ Check 4: Processors ? Learn more	
 ▶ Check 5: Disk Space Available ? Learn more	
 ▶ Check 6: Memory Available ? Learn more	
 ▶ Check 7: Software Required ? Learn more	
 ▶ Check 8: Port Availability ? Learn more	
 ▶ Check 9: Upgrade Check ? Learn more	
 ▶ Check 10 IPMI Status ? Learn more	
IPMI needs to be installed and enabled for IBM Systems Director to function properly.	
Return Code:	WARN Return Code: 34
Warning:	IPMI status could not be determined; error returned from native environment request.
Required:	The system you are installing may not have the IPMI (Intelligent Platform Management Interface) kernel modules or may not have a BMC (Baseboard Management Controller). You may not receive certain hardware events.
 ▶ Check 11 SELinux Status ? Learn more	
 ▶ Check 12: Migration Information ? Learn more	
 ▶ Check 13: Performance Information ? Learn more	
 ▶ Check 14: User Name Check	
 ▶ Check 15: RSA Check ? Learn more	
 ▶ Check 16: Swap Space Check ? Learn more	
 ▶ Check 18: Umask Check ? Learn more	
 ▶ Check 19: Host Name Resolution Check ? Learn more	
 ▶ Check 20: File Path Check	
 ▶ Check 23: Post-Installation Validator Check	

Figure 1-12 Pre-installation check result

If you run your system from the command line, the report is in text format and looks similar to the output in Figure 1-13.

```
Java:
/isd632/standard_linux_x86_Director_base/server/checkds/jvm/xlinux/bin/java

Starting IBM Systems Director Pre-Installation Utility...
Finished analysing system
Creating reports...

Install Readiness Text report being written to
  /tmp/checkds/reports/checkDS_Text_20121214_174936.txt
Install Readiness Error Text report being written to
  /tmp/checkds/reports/checkDS_Error.txt
Install Readiness Detailed HTML report being written to
  /tmp/checkds/reports/checkDS_Detailed_20121214_174936.html
Install Readiness Summary HTML report being written to
  /tmp/checkds/reports/checkDS_Summary_20121214_174937.html

Your system is currently showing warnings for 1 of 21 checks.

WARN Check 10 IPMI Status

IPMI status could not be determined; error returned from native environment request.

The system you are installing may not have the IPMI (Intelligent Platform Management
Interface) kernel modules or maynot have a BMC (Baseboard Management Controller).

You may not receive certain hardware events.

Overall Report Return Code: 34
```

Figure 1-13 Text output from the pre-installation utility

If recommendations or errors exist, you must address them before you can continue the installation. For information about the problems, see the report. After the problems are fixed, run the pre-installation check again.

4. To install the Systems Director server, from within the directory of the installation script, type one of the following commands and press Enter:
 - To accept the default settings, enter this command:
`./dirinstall.server`
 - To use the response file, enter this command:
`./dirinstall.server -r /directory/response.rsp`
The *directory* is the local directory to which you copied the response file and *response.rsp* is the name of the response file.
 - To force a clean installation, regardless of the existing data, enter this command:
`./dirinstall.server -g`

Tip: If you previously installed Systems Director on this system, data is saved in the /var/tmp/director_save_630 directory, by default. The data is not removed even if you uninstall the previous installation. If you want a clean installation, use `./dirinstall.server -g` to ensure that you do not inadvertently migrate this data. Systems Director 6.3.x installs cleanly and the data from the previous installation is preserved.

5. The installation runs now with the default setting or with the settings from the response file. If you use the default integrated DB2 database, the installation automatically creates the settings to use DB2. If you use another supported database, you must configure the database for use with Systems Director.

For information about how to configure these databases, see the IBM Systems Director Information Center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.configdir.helps.doc%2Ffqm0_t_config_database_application_cfgdbcmd.html

6. First, the license agreement is displayed. Confirm that you accept this agreement by entering 1. The Pre-Installation Utility runs. In our example, we got the return code 34. Return code 34 means that no IPMI Driver is installed. However, we run in a virtual environment, so there is no problem. Enter 1 to continue as shown in Figure 1-14.

```
Sles11:/ # ./tmp/isd632/server/dirinstall.server
Agree to product licence?
[1-Agree | o-Disagree]: 1
IBM Systems Director 6.3.2 installation
.....
Starting IBM Systems Director Pre-Installation Utility ...
.....
Overall Report return Code:34
For more details see the files under /tmp/checkds
[1-Continue | 0-Abort]: 1
....
```

Figure 1-14 Running dirinstall.server script

7. The Director server, components, features, and embedded DB2 database are installed. When the installation completes, a message appears that is similar to the following message from our installation (Figure 1-15).

```
...
Installation of the IBM Systems Director Server 6.3.2 succeeded

To start the server manually, run /opt/ibm/director/bin/smstart
To see the status, run /opt/ibm/director/bin/smstatus [-r]
Sles11:/ #
```

Figure 1-15 Completing the Systems Director installation

8. After the installation completes, configure the Agent Manager and then start the Systems Director.

Important: Do not start the Systems Director before you configure the Agent Manager.

9. To configure the Agent Manager (if you did not configure it during the installation process), run the following command:

```
install_root/bin/configAgtMgr.sh
```

10. Respond to the `configAgtMgr.sh` script prompts:

- Agent Manager

Enter 1 to use the Agent Manager that is installed with this server (suggested), or enter 0 to use an existing Agent Manager (advanced).

- Resource Manager

Enter the Resource Manager user ID that you want to set for the Agent Manager. The user ID does not need to be an operating system user ID. Remember this user ID. If you want to use the same Agent Manager with another system, you need this user ID.

Enter and verify the Resource Manager password to set for the Agent Manager.

- Agent Registration password

Enter and verify the Agent Registration password to set for your Agent Manager. This password can be the same password for the Agent Manager. This password is used to register the Common Agents with Agent Manager.

- IP address and port for Agent Manager

Enter the IP address for the existing Agent Manager.

If you selected 0 (use an existing Agent Manager), you must provide the IP address of the existing Agent Manager.

Enter the port number for the existing Agent Manager.

If you selected 0 (use an existing Agent Manager), you must provide the port number of the existing Agent Manager. The port number must be a valid number 0 - 65535.

11. Start Systems Director processes on the management servers by running the `smstart` command:

```
install_root/bin/smstart
```

12. To check the status of the Systems Director, run the following command:

```
install_root/bin/smstatus -r
```

When this command returns a value of Active, the server is started.

1.5.3 Installation on Windows

To install the Systems Director server on a Windows server, follow these steps:

1. Download the installation package from the following link and uncompress it:
<http://ibm.com/systems/software/director/downloads/mgmtservers.htm>
2. Double-click the `IBMSystemsDirectorServerSetup64.exe` file to start the installation process.
3. The pre-installation check runs. If the check runs successfully, you see a green mark and the “No warnings or errors were found” message (Figure 1-16 on page 21). Click **Next**

to continue. If problem and error messages appear, fix them, return to this window, and run the installation program again.



Figure 1-16 Welcome to the InstallShield wizard for Systems Director Server 6.3.2

4. Agree to the license agreement and click **Next** to continue.
5. Specify the folder where you want to install the software (Figure 1-17) and click **Next** to continue.

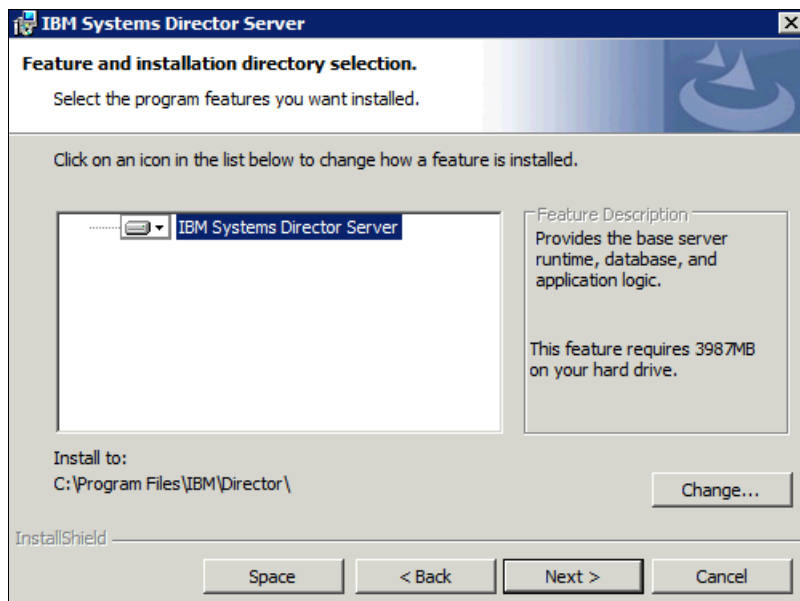


Figure 1-17 Feature and installation directory selection

6. In the next window (Figure 1-18), select the installation type. Two types are available:
- Click **Basic** to use the embedded database and default ports and install the Common Agent Services (CAS) server with the director installation. You type the user ID and password only one time. The installation program uses the user ID and password for all settings.
 - Click **Advanced** if you want to use another database and the embedded, managed DB2. Also, if you install a second Systems Director server in your environment, use the Advanced setup to select the existing CAS server. With the Advanced setup, you can define a different user ID and password for the CAS server. With the Advanced setup, you can use different default ports for the Systems Director server.

For our installation, we use the Basic setup type. Click **Next** to continue.

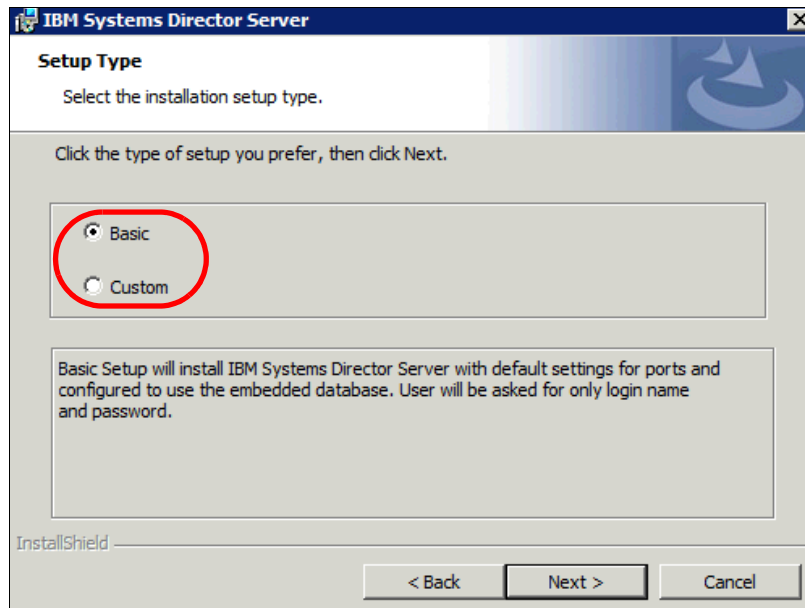


Figure 1-18 Setup type

7. Enter in the credentials that you want to use for the Systems Director server: computer name, user name, and password (Figure 1-19). Click **Next** to continue.

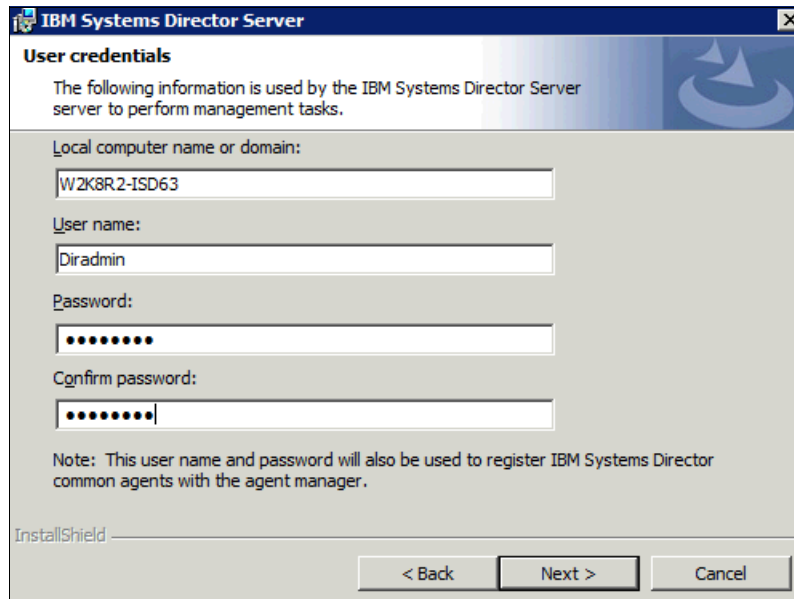


Figure 1-19 User credentials

8. After you are ready to begin the installation process, click **Install** (Figure 1-20).

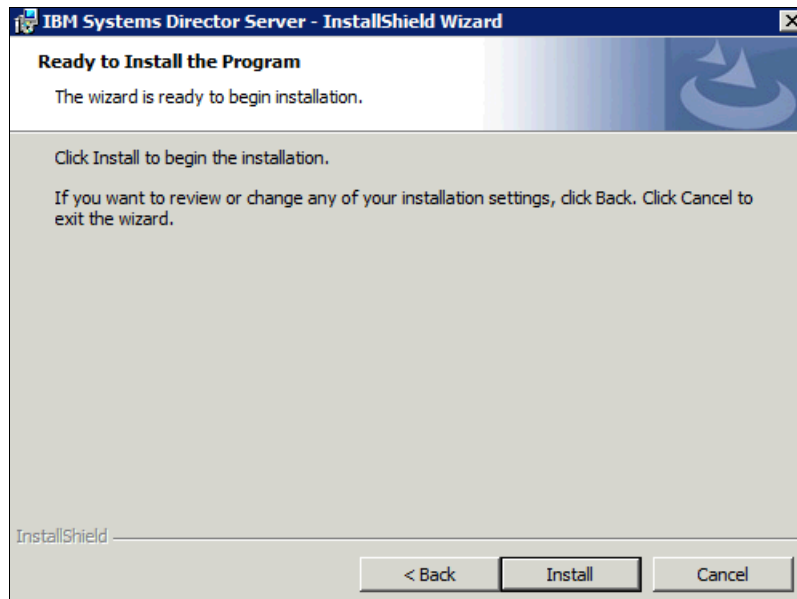


Figure 1-20 Ready to Install the Program

9. The Systems Director server database is installed. You can see the progress of the installation process (Figure 1-21).

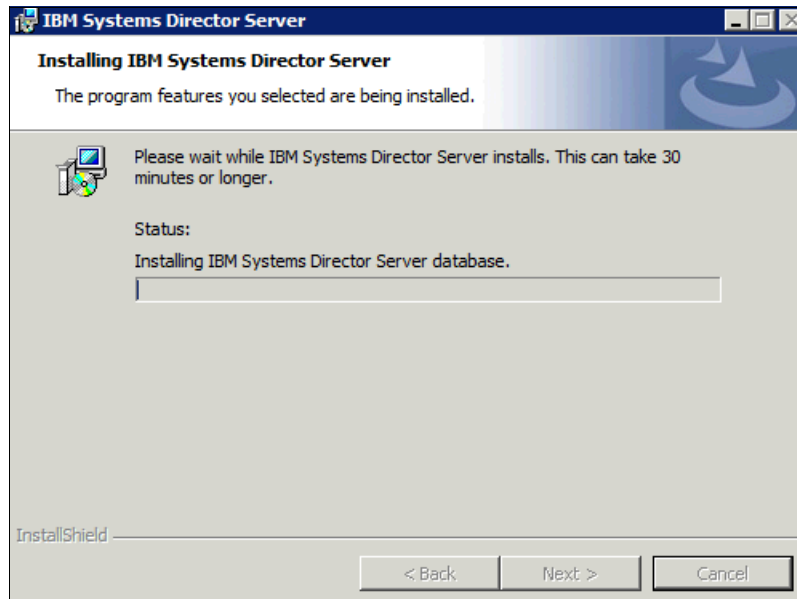


Figure 1-21 Installing the Systems Director server

10. The Systems Director Common Agent is installed next (Figure 1-22).

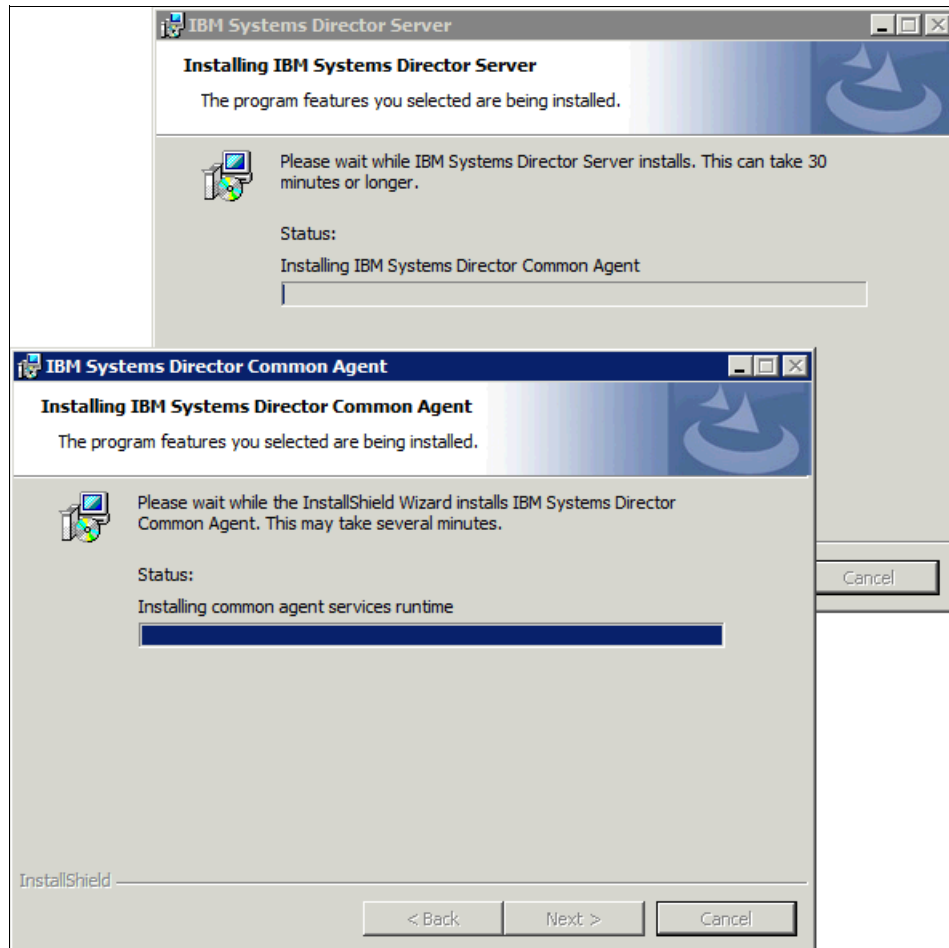


Figure 1-22 Install Common Agent and Common Agent services

11. The Systems Director Platform Agent packages are installed (Figure 1-23).

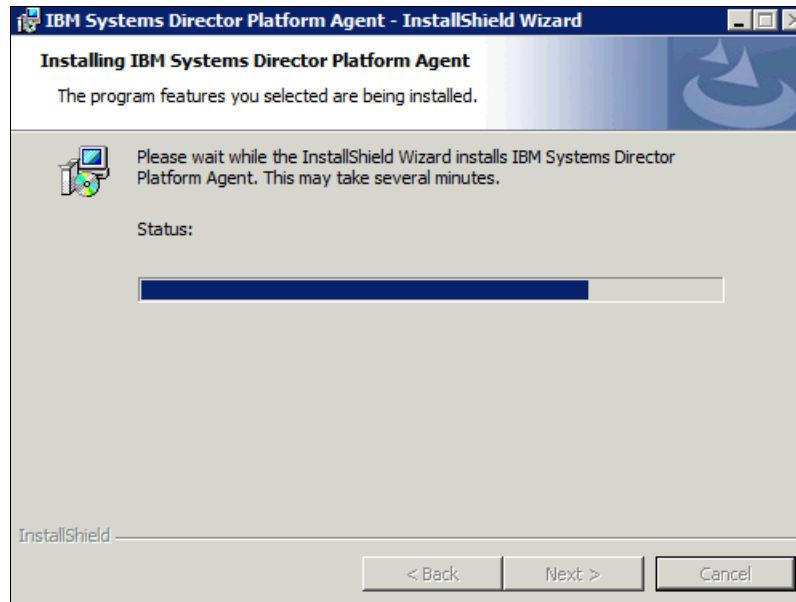


Figure 1-23 Platform Agent installation

12. The files for the Systems Director server are installed (Figure 1-24).

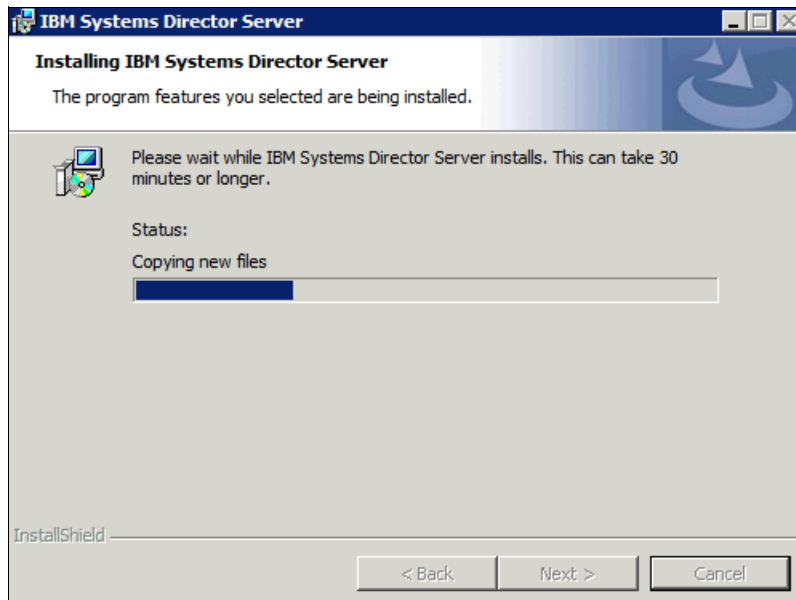


Figure 1-24 Installing the Systems Director server

13. Additional features and plug-ins are installed (Figure 1-25).

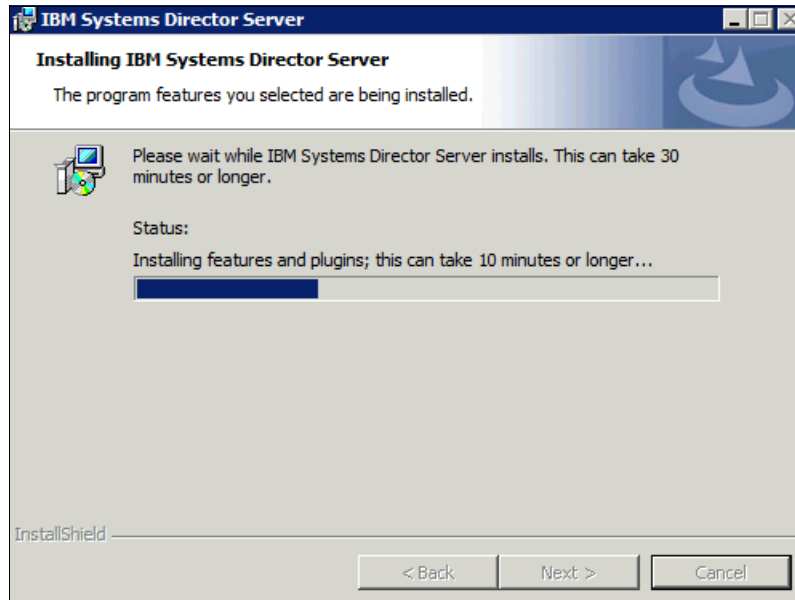


Figure 1-25 Installing features and plug-ins

14. The Agent Manager (CAS server) is installed (Figure 1-26).

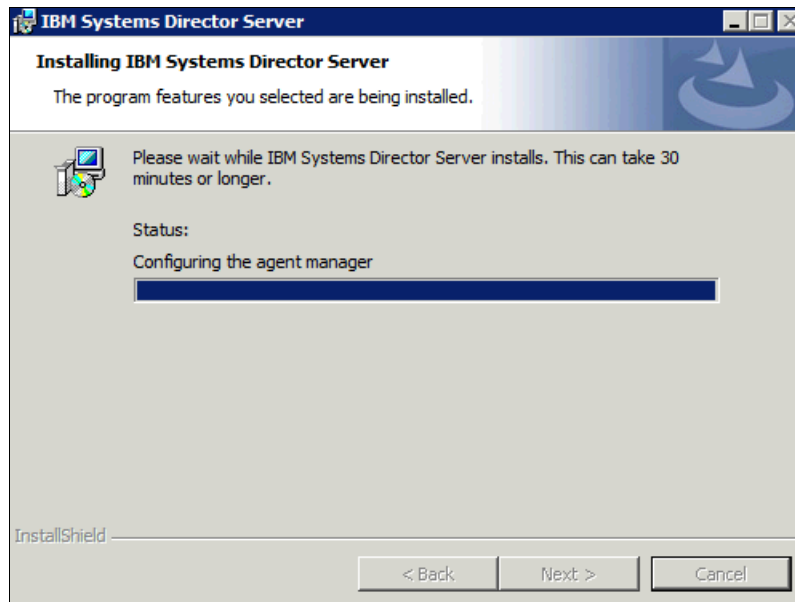


Figure 1-26 Installing Agent Manager

15. When the installation completes, the InstallShield wizard Completed window opens (Figure 1-27). You can view the Windows Installer log. Complete the installation by clicking **Finish**.

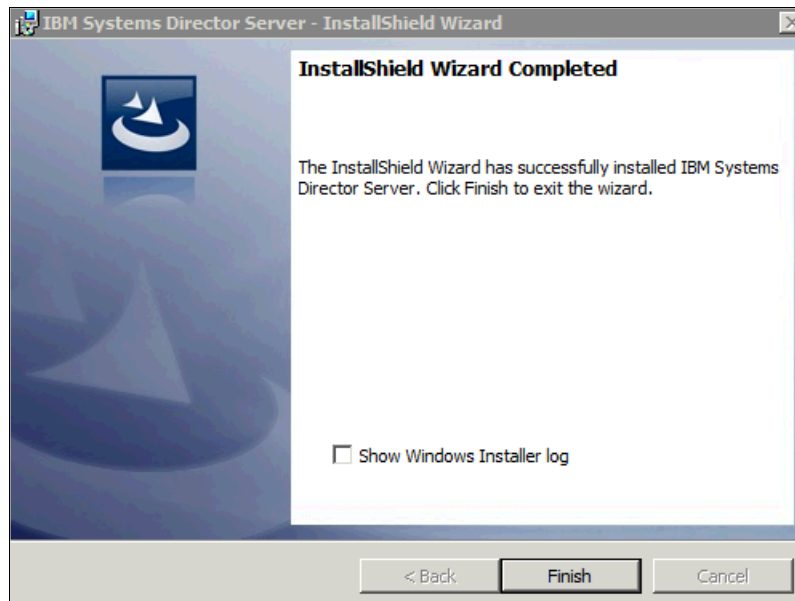


Figure 1-27 InstallShield wizard Completed window

After the installation is finished, the Systems Director server starts automatically. You can check the status of the Systems Director server through the status icon or by using the **smstatus -r** command. When the status icon shows a green circle or the status shows as active, the Systems Director server is up and running.

1.5.4 Post Installation Validation (PIV) tool

With Systems Director 6.3.2, IBM provides the new Post Installation Validation (PIV) tool. This tool can be run after the installation process to check the installation for completeness and errors. The tool is in the `/piv` folder in the installation medium or directory.

The PIV analyzes the installation logs for errors and checks for services, ports, Agent Manager configuration, and database configuration. The PIV also checks whether the server is active by using the **smstatus** command.

The PIV tool is small (less than 5 MB). The PIV tool is written in Python and includes a small Python interpreter. (Python must be installed on the system to run PIV.) PIV is not a health checker for a running Systems Director; it is only a tool to verify the installation.

The tool is a command-line tool and is run in the following way:

- ▶ Linux on x86:

```
<Install_directory>\bin\piv> .\PostInstallValidator_xLin.sh
```
- ▶ Windows:

```
<Install_directory>\bin\piv> .\PostInstallValidator_Win.exe
```

Command options are available. You can see the full list of command-line options by using the **-h** option.

The following command options are the most important options:

-o or --output	Specify the location of the installation report
-c or --config	Specify the location of the configuration file
-s or --silent	Run the tool silently
-r or --report	Open the text report on completion (Windows only)
-j or --nohtmlreport	Do not create an HTML report
-d or --detailed	Include detailed information in the report
-w or --wait	Wait to return until the installation is completed

The tool generates a report. If a GUI is available, you receive an HTML report (if not, clear by using the **-j** option). If only a command-line environment is available, you receive a text report.

The reports are in the following directories, by default:

- ▶ Linux/AIX reports are in the `/tmp` directory.
- ▶ Windows reports are in the `%temp%` directory.

The PIV HTML report looks similar to the example of our installation in Windows Server 2008 R2 x64 (Figure 1-28 on page 30).

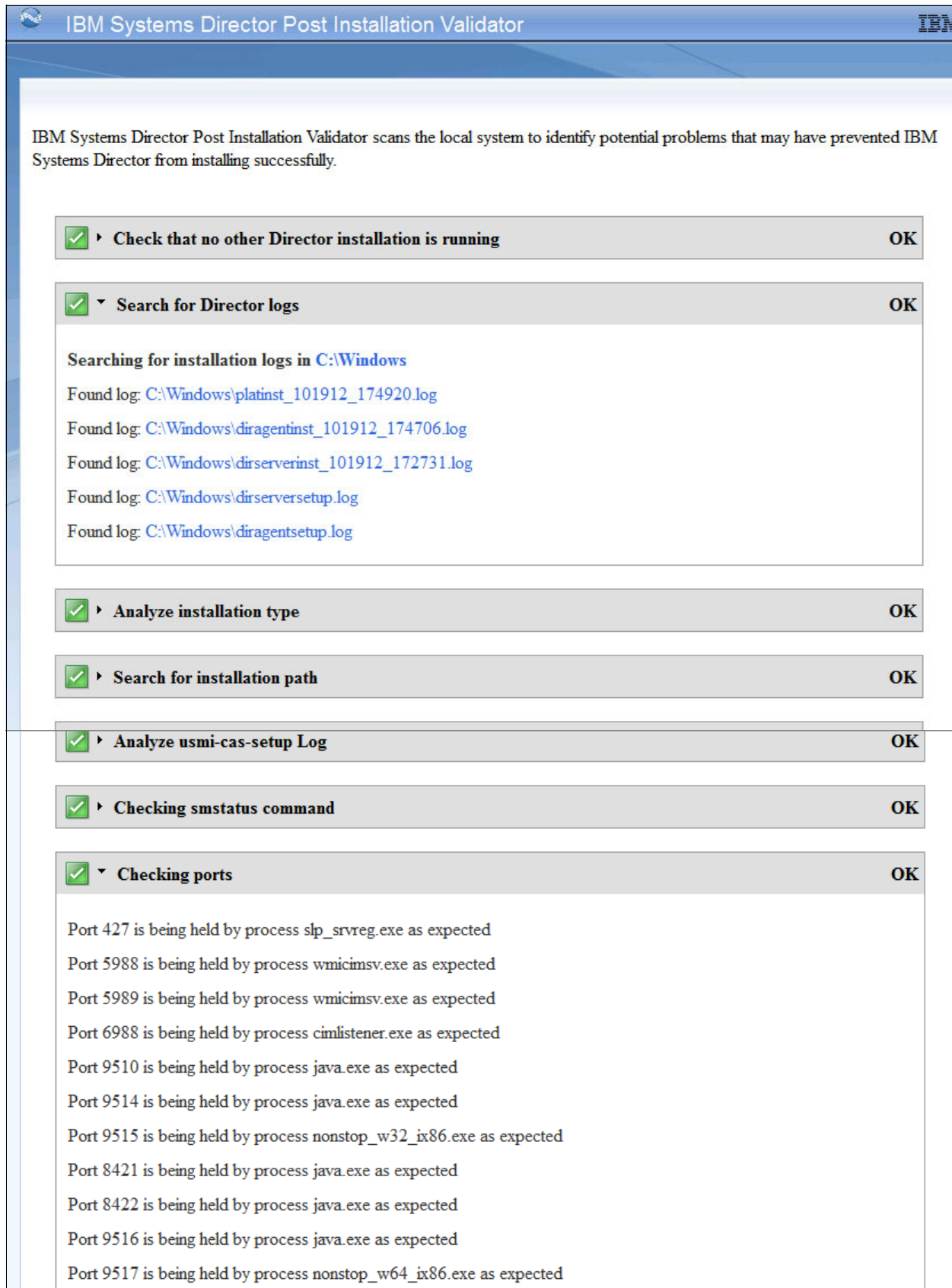


Figure 1-28 PIV HTML report

The text report looks similar to the following report from our installation (Figure 1-29).

```
PS <C:\Program Files\IBM\Director\bin\piv> .\PostInstallValidator_
win.exe
Report being written to c:\users\Administrator\appdata\local\temp\PostInstallationReport.txt
Loading configuration file ./piv.ini
Check that no other Director installation is running.....OK
Search for Director logs.....OK
Analyze installation type.....OK
Search for installation path.....OK
Verify install directory.....OK
Analyze windows Server MSI log file.....OK
Analyze windows Common Agent MSI log file.....OK
Analyze windows Server log file.....OK
Analyze windows TivGuid MSI log file.....OK
Analyze windows Tivoli CAS Pre-Install log file.....OK
Analyze windows Tivoli CAS Install status log file.....OK
Analyze windows Tivoli CAS Install status log file.....OK
Analyze windows Platform Agent MSI log file.....FAIL
Check that the Agent Manager is configured.....OK
Search for configuration logs.....OK
Analyze InstallFeatures log.....OK
Analyze InstallConfigTools Log.....OK
Analyze InstallConfigTools Log 1.....OK
Check database install configuration.....OK
Analyze smreset.log.....OK
Analyze reset.log.....OK
Analyze mergetools.log.....OK
Analyze mergetools.log.1.....OK
Analyze mergetools.log.2.....OK
Analyze usm1-cas-setup Log.....OK
Checking smstatus command.....OK
Checking ports.....OK
Checking active services.....OK
Analyze PIU results.....OK
Press return to exit
```

Figure 1-29 PIV text report

1.5.5 Starting Systems Director

The Systems Director automatically starts after the installation. No reboot of the system is necessary. You can start and stop the Systems Director server by using the command line. The command line is the best method because all necessary services are started and stopped in the correct sequence.

Use the following commands to start or stop Systems Director:

- ▶ Linux:
 - **smstart** to start the Systems Director server
 - **smstop** to stop the Systems Director server
- ▶ Windows
 - **net start dirserver** to start the Systems Director server
 - **net stop dirserver** to stop the Systems Director server

Initial logon

After the IBM Systems Director server is in the active status, you can log on to the Systems Director web interface:

1. Open your browser and type in the following address:

http://hostname_or_IP_address:8421/ibm/console/logon.jsp

or

https://hostname_or_IP_address:8422/ibm/console/logon.jsp

- At the first access, a window opens to show you that the connection is untrusted (Figure 1-30). Click **Add Exception**.

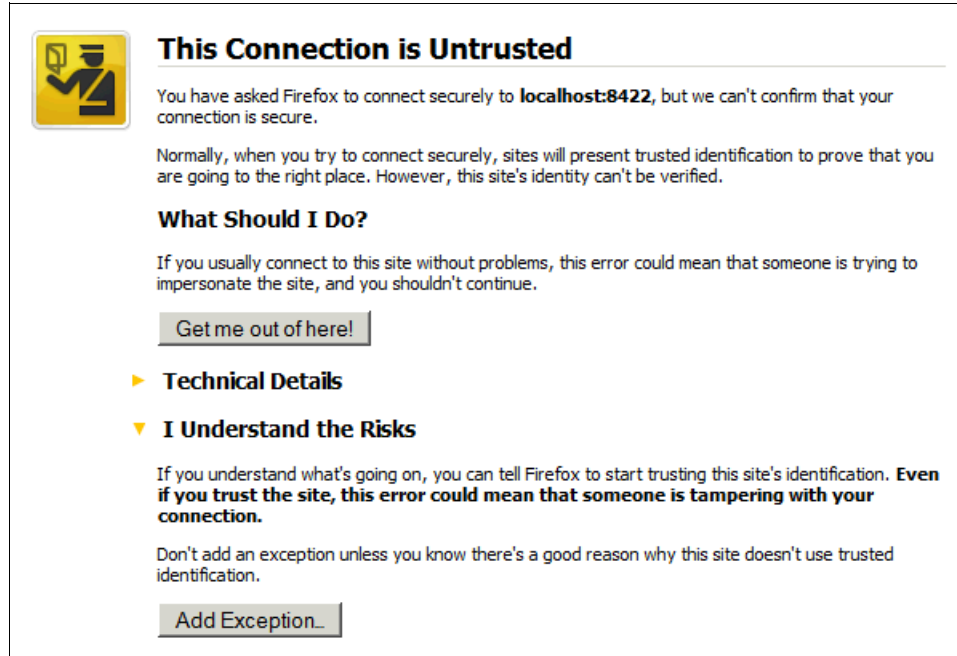


Figure 1-30 Untrusted connection

- A new window opens (Figure 1-31). Click **Confirm Security Exception**.

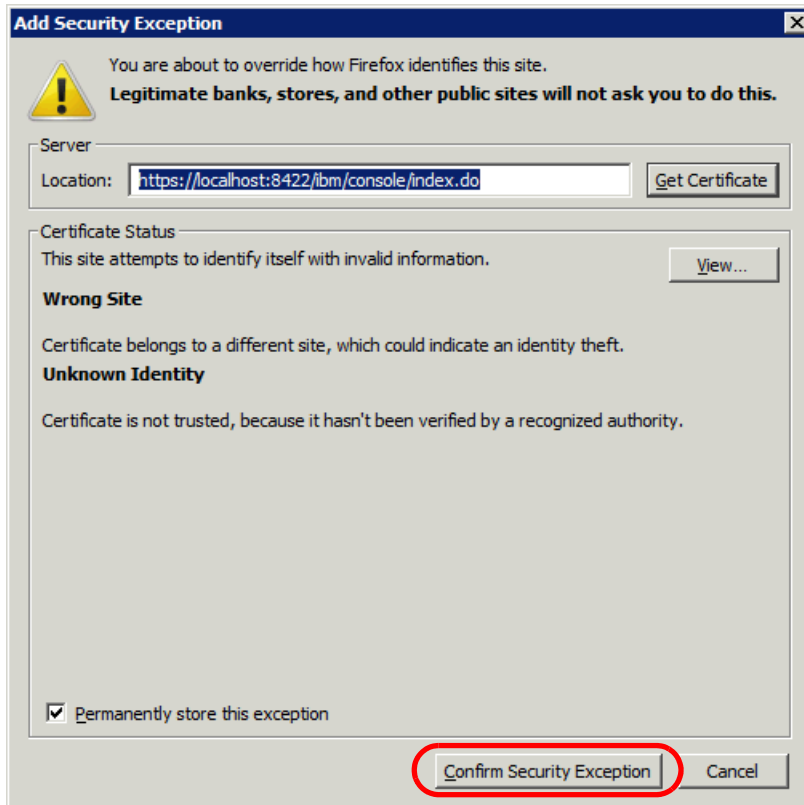


Figure 1-31 Confirm Security Exception

4. The logon window opens (Figure 1-32).



Figure 1-32 Logon pane

1.6 Installing Systems Director on an AIX platform

Useful information about the process of installing Systems Director on an AIX platform is described.

Resources that are required for running the Systems Director server are referenced in 1.2, “IBM Systems Workload Estimator” on page 2 and 1.3, “System resources” on page 7.

For the installation of Systems Director on AIX, read the following information:

http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.director.install.helps.doc/fqm0_t_installing.html

The Systems Director Management server code can be sourced from the following URL:

<http://www-03.ibm.com/systems/software/director/downloads/mgmtservers.html>

1.6.1 Downloading the software

The Systems Director source can be downloaded in two formats: an .iso file or a GZIP (.gz) file. Download your preferred file type and place it in a temporary file system on the AIX server:

► ISO:

```
loopmount -i express_aix_Director_base.iso -o “-V cdrfs -o rw” -m /mnt
```

► GZIP:

```
gunzip -c express_aix_Director_base.tar.gz | tar -xvf -
```

The installation of the Systems Director server comes with an embedded pre-installation check utility. This option is enabled, by default, and is referenced in the `dirserv.rsp` file. The suggestion is to leave the pre-installation check enabled, which is the default (Figure 1-33).

```
Variables will be used during the installation:
PRE_INSTALL_CHECKS : 1
```

Figure 1-33 Pre-installation checks are enabled by default in the `dirserv.rsp` file

The preferred practice is to also run the `checkds` utility before you run `dirinstall.server`. The `checkds.sh` script is in the server folder:

```
/mnt/server/checkds/checkds.sh
```

On successful completion of the `checkds` script, proceed with the installation.

1.6.2 Prerequisites

For the installation, complete the following checks in any order before the installation of Systems Director.

Yellow pages

Ensure that the yellow pages group is not running and is in an inoperative state (Figure 1-34). Otherwise, the embedded DB2 for the Systems Director server does not install successfully.

```
-bash-3.2# lssrc -s ypbind
Subsystem      Group      PID      Status
ypbind         yp         0        inoperative
```

Figure 1-34 Yellow pages

OS level

Check that the OS level of the AIX server is supported:

http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.director.plan.helps.doc/fqm0_t_planning_to_install_ibm_director_server.html

ulimits

Ensure that the `fsize` setting is set to unlimited because `fsize` determines the maximum allowable file size.

```
vi /etc/security/limits
default:
    fsize = -1
```

Figure 1-35 `ulimits`

The Systems Director installation file is larger than 2 GB. Log out of the terminal session to activate the `fsize` changes.

Required installation files

Ensure that the filesets for AIX are installed for Secure Shell (ssh) and Secure Sockets Layer (ssl) at the following level or greater. See Figure 1-36.

```
-bash-3.2# lsllp -L | egrep "ssh|ssl"
  openssl.base.client      5.0.0.5302  C   F   Open Secure Shell Commands
  openssl.base.server     5.0.0.5302  C   F   Open Secure Shell Server
  openssl.license         5.0.0.5302  C   F   Open Secure Shell License
  openssl.base            0.9.8.801   C   F   Open Secure Socket Layer
  openssl.man.en_US       0.9.8.1800  C   F   Open Secure Socket Layer
-bash-3.2#
```

Figure 1-36 ssh/ssl filesets

Check that no previous installation of Systems Director exists (Figure 1-37). If a previous installation exists, uninstall it.

```
lsllp -l | egrep -i "directorserver|directorcomm|directorplat|cimserver|cas"
```

Figure 1-37 lsllp check

If filesets from a previous installation are returned or for the filesets that are listed in Figure 1-36, remove the associated files (Figure 1-38).

```
installp -ug DirectorServer DirectorCommonAgent DirectorPlatformAgent cas.rte
sysmgt.cimserver.pegasus.rte
```

Figure 1-38 installp -ug

If a service is locked and cannot be removed, use the **lsof** or **rmsock** command to determine which port or file prevents the removal of the associated files. Then, remove the filesystems that are associated to the files (Figure 1-39).

```
rm -rf /opt/ibm/director
rm -rf /opt/ibm/icc
rm -rf /opt/ibm/tivoli
```

Figure 1-39 folder removal

Filesets: It is not compulsory to remove the filesets that are referenced with the **-ug** option. However, by removing these filesets, you eliminate any issues with previous installations for Agents or the server, which leads to a smoother installation.

Volume groups

The suggestion is to leave rootvg primarily for the operating system. Create a separate volume group for the additional storage that is required for Systems Director on an alternate disk. By keeping rootvg lean and clean, you can recover more easily. The Systems Director server recovery is described in Chapter 4, "Backup" on page 219.

Because the DB2 installation is restricted, the DB2 installation path is also restricted (Figure 1-40).

```
/home/dirinst1
/opt/ibm/director/db2
```

Figure 1-40 DB2 default paths

Changing this path to an alternate path for the system backup and restoration of rootvg is beneficial (Figure 1-41).

```
mklv -y "isddb2" -t jfs2 rootvg 10G
crfs -v jfs2 -d isddb2 -m /isddb2 -A yes
mount /isddb2
```

Figure 1-41 Changing the path

Tip: Our installation has only one disk. It is advisable to have n+1 and to mirror the volume groups that are associated to the disks. Repeat the commands in Figure 1-41 for /opt/ibm/director on the alternate volume group if you want.

The **checkds** script looks for 3 GB or greater of paging space (Figure 1-42).

```
-bash-3.2# lsps -a
Page Space Physical Volume Volume Group Size %Used Active Auto Type Chksum
hd6 hdisk0 rootvg 1024MB 2 yes yes lv 0
-bash-3.2# chps -s 2 hd6
-bash-3.2# lsps -a
Page Space Physical Volume Volume Group Size %Used Active Auto Type Chksum
hd6 hdisk0 rootvg 3072MB 1 yes yes lv 0
```

Figure 1-42 Paging space

1.6.3 Installation

Because the iso is mounted on /mnt, we changed the path to /mnt/server/, which is the location of the **dirinstall.server** executable script. Before you run the installation script, change the default DB2 path of the database. Because the media is mounted in read-only mode, copy the file to a temporary directory. Edit the **dirsrv.rsp** file with a text editor. Figure 1-43 shows the database path that we chose for the installation. It is referenced by the **DB_DATAPATH** variable.

```
# Used to specify where the managed DB2 database will be stored when
# managed DB2 database is selected. If not specified the default path will be
# /home/dirinst1. If the path does not exist, it will be created.
DB_DATAPATH=/isddb2
```

Figure 1-43 dirsrv.rsp

When you start the installation for Systems Director, name the executable the name that is shown in Figure 1-44 to point to the changed response file.

```
-bash-3.2# ./dirinstall.server -r /tmp/dirserv.rsp
+-----+
Start of product installation on SA-W217-1AIX
+-----+
Variables will be used during the installation:
  PRE_INSTALL_CHECKS : 0
  PortNumber : 8421
  SecurePortNumber : 8422
  AGENT_MANAGER_PORT : 20000
  MIGRATE_DATA : 1
  UPDATES_PATH : /mnt/server/packages/updates
  -Managed DB2 is supported and its prerequisites are met.
  DB_INST_TYPE : 1
  DB_DATAPATH : /isddb2
  DB_PWD : default.
  DB_INSTANCEPATH : .
  DB_SERVER : localhost
  DB_PORT : default
+-----+
```

Figure 1-44 Specifying a response file

Successful installation is similar to Figure 1-45.

```
Attempting to install features.....done
Stopping the server runtime...done
Configuring database.....done
Finished processing all filesets. (Total time: 45 mins 48 secs).
Finished processing all filesets. (Total time: 45 mins 51 secs).

+-----+
Summaries:
+-----+

Installation Summary
-----
Name                    Level      Part      Event      Result
-----
DirectorServer          6.3.0.0   USR       APPLY      SUCCESS
DirectorServer          6.3.0.0   ROOT      APPLY      SUCCESS
Installation of IBM Systems Director Server completed successfully.
This installation log file can be found in /var/log/dirinst.log.
You must configure the agent manager prior to starting the server.
To configure the agent manager, run
/opt/ibm/director/bin/configAgtMgr.sh
To start the server manually, run
/opt/ibm/director/bin/smstart
```

Figure 1-45 Successful installation

The Agent Manager provides authentication and authorization services for managed systems that have common installed agents:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_configAgtMgr.html

As shown in Figure 1-45 on page 37, the Agent Manager must be configured before you start the Systems Director server. See Figure 1-46.

```
/opt/ibm/director/bin/configAgtMgr.sh
-bash-3.2# /opt/ibm/director/bin/configAgtMgr.sh
Enter 1 to use the Agent Manager installed with this server (recommended)
Enter 0 to use an existing Agent Manager (advanced) : 1
Enter Resource Manager username : itso
Enter Resource Manager password :isd4itso
Re-Enter Resource Manager password :
Enter Agent Registration password :
Re-Enter Agent Registration password :
Re-Enter Agent Registration password :
[Add] [Element]: AgentManagerUserID [Value]: itso
[Add] [Element]: AgentManagerPassword [Value]:
{aes:3C5SnKQL63SjkEy44Gs+vHE6nQzC+Di11NzNvSiAzk=}fFn7zXZpwwH3wYuP1yCIw==
[Add] [Element]: ManagerRegistrationPassword [Value]:
{aes:3C5SnKQL63SjkEy44Gs+vHE6nQzC+Di11NzNvSiAzk=}fFn7zXZpwwH3wYuP1yCIw==
DataSourceConfig.sh=0
DataStoreInstall.sh=0
GenerateCertificates.sh=0
EncryptAMProps.sh=0
WebConfig.sh=0
usmi-cas-setup.sh=0
-bash-3.2#
```

Figure 1-46 Agent Manager configuration

The return codes of all called scripts must be 0. Because all tasks are now successfully completed, we start Systems Director (Figure 1-47).

```
-bash-3.2# export /opt/ibm/director/bin
-bash-3.2# export PATH=$PATH:/opt/ibm/director/bin
-bash-3.2# smstart
Starting IBM Director...
The starting process may take a while. Please use smstatus to check if the server is
active.
-bash-3.2# smstatus -r
Starting
Active
```

Figure 1-47 Starting Systems Director

We confirm that the server returned an Active state. Now, we can change the DB2 parameters that relate to the system setup, if necessary.

1.6.4 DB2 settings

Disabling remote access for the DB2 user is not required. However, it helps to prevent issues with user IDs and in-house AIX security policies:

<http://www-01.ibm.com/support/docview.wss?uid=isg1IC83082>

Stop Systems Director and make the following changes:

1. Stop the Systems Director server (Figure 1-48).

```
-bash-3.2# smstop
Shutting down IBM Director...
```

Figure 1-48 Stopping Systems Director

2. Edit the user file (Figure 1-49).

```
-bash-3.2#vi /etc/security/user
dirinst1:
    admin = false
    rlogin=false
```

Figure 1-49 Edit the user properties file

3. Edit the sshd_config file (Figure 1-50).

```
vi /etc/ssh/sshd_config
# Added to restrict remote access
DenyUsers  dirinst1
```

Figure 1-50 Edit the sshd_config file

4. Restart sshd (Figure 1-51).

```
-bash-3.2# stopsrc -s sshd
0513-044 The sshd Subsystem was requested to stop.
-bash-3.2# startsrc -s sshd
0513-059 The sshd Subsystem has been started. Subsystem PID is 16973974.
-bash-3.2#1
```

Figure 1-51 Restart sshd

5. Restart Systems Director (Figure 1-52).

```
-bash-3.2# smstart
Starting IBM Director...
The starting process may take a while. Please use smstatus to check if the server is
active.
```

Figure 1-52 Restart Systems Director

Because the response file for the DB2 installation is customized, check whether the database path is configured as requested in the response file. Figure 1-53 shows file system usage.

```
df -g
-bash-3.2# df -g /home/dirinst1 /isddb2
Filesystem      GB blocks      Free %Used      Iused %Iused Mounted on
/dev/hd1         2.00          1.95   3%         211      1% /home
/dev/isddb2      10.00         9.31   7%         104      1% /isddb2
```

Figure 1-53 File system usage

By using **db2** commands, query the database parameters to confirm the path within DB2 (Figure 1-54).

```
-bash-3.2# su - dirinst1
$ db2 get dbm config | grep "database pa"
Default database path                (DFTDBPATH) = /isddb2
$
```

Figure 1-54 DB2 path

Changing the default database path after the installation: During the installation, you might not edit the `dirserv.rsp` file. You can change the default database path after the installation by using the **db2relocatedb** command. This command does not require a backup and restore. For more information, see the information center:

<http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.cmd.doc%2Fdoc%2Fr0004500.html>

Because Systems Director is installed and no endpoint discoveries or additional tasks are complete, back up Systems Director in its current state. Before you complete the save, create another lv, fs, and mount. Or, use the **smssave** command.

Optionally, create another mount point to point the **smssave** to an alternate directory (Figure 1-55).

```
mk1v -y "isdbkup" -t jfs2 rootvg 10G
crfs -v jfs2 -d isdbkup -m /isdbkup -A yes
mount /isdbkup
```

Figure 1-55 Back up lv and fs

After you create another mount point, run **smssave** with options (Figure 1-56).

```
-bash-3.2# smstop;smssave -targetDir /isdbkup
Shutting down IBM Director...
Command is running. Monitor live status and results in /opt/ibm/director/log/smsave.log

ALR1325I: The lightweight runtime has started.
com.ibm.net.SocketKeepAliveParameters

Command completed successfully
```

Figure 1-56 The **smssave** command with options

Figure 1-57 shows the `smssave` command with no options is shown in.

```
-bash-3.2# smstop;smssave;smstart
Shutting down IBM Director...
Command is running. Monitor live status and results in /opt/ibm/director/log/smsave.log
ALR1325I: The lightweight runtime has started.
com.ibm.net.SocketKeepAliveParameters
Command completed successfully
Starting IBM Director...
The starting process may take a while. Please use smstatus to check if the server is
active.
-bash-3.2# smstatus
Active
```

Figure 1-57 `smssave` with no options

Figure 1-58 shows the location of both backups.

```
-bash-3.2# ls -al /isdbkup
total 8
drwxr-xr-x  4 root    system    256 Nov 07 11:27 .
drwxr-xr-x 26 root    system    4096 Nov 07 10:40 ..
drwxr-xr-x  8 root    system    256 Nov 07 11:30 2012_11_7_11.27.1
drwxr-xr-x  2 root    system    256 Nov 07 10:40 lost+found
-bash-3.2# ls -al /opt/ibm/director/backup
total 8
drwxr-xr-x  3 root    system    256 Nov 07 11:30 .
drwxr-xr-x 30 root    system    4096 Oct 22 14:30 ..
drwxr-xr-x  8 root    system    256 Oct 22 14:32 2012_10_22_14.29.29
-bash-3.2#
```

Figure 1-58 Location of backups

Systems Director backups are discussed in Chapter 4, “Backup” on page 219.

1.6.5 Initial login

After you successfully start Systems Director, log in to the server through the user interface (UI) as shown in Figure 1-59 on page 42.

In our example, `SA-W217-1AIX.itso.ra1.ibm.com` is the host name of the server where Systems Director is installed. Or, use the native IP address of the server. We used this URL:

`https://SA-W217-1AIX.itso.ra1.ibm.com:8422/ibm/console/logon.jsp`

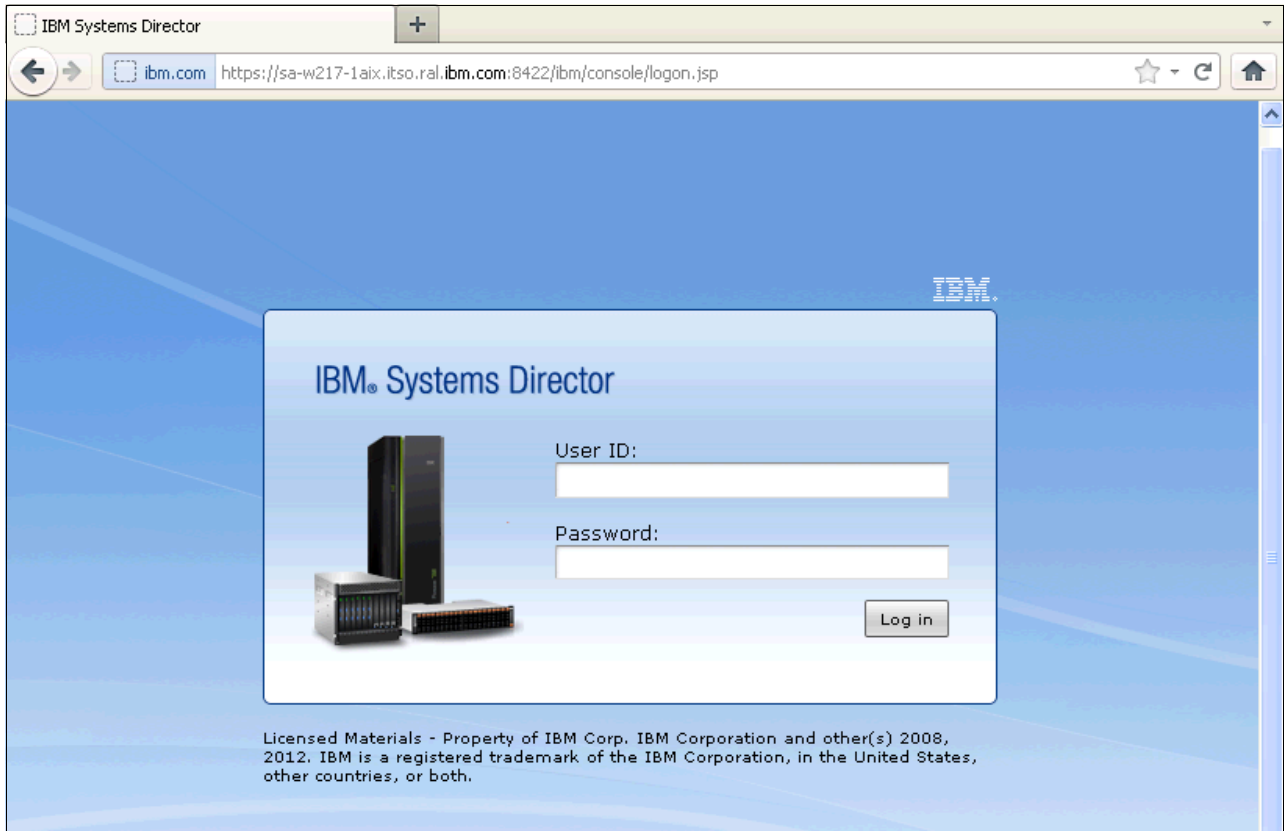


Figure 1-59 IBM Systems Director login panel

After you log in to Systems Director, select the **Plug-ins** tab. Select **IBM Systems Director Server** to get an overview of the server and associated properties (Figure 1-60).



Figure 1-60 Systems Director Server

1.6.6 Installing the Systems Director license

The Systems Director license is on the root path of the ISO or GZIP file that you transferred to the installation server. The license key can be imported by using the command line. Or, use the UI for a license key that is stored locally on the computer that is used to access the UI (Figure 1-61).

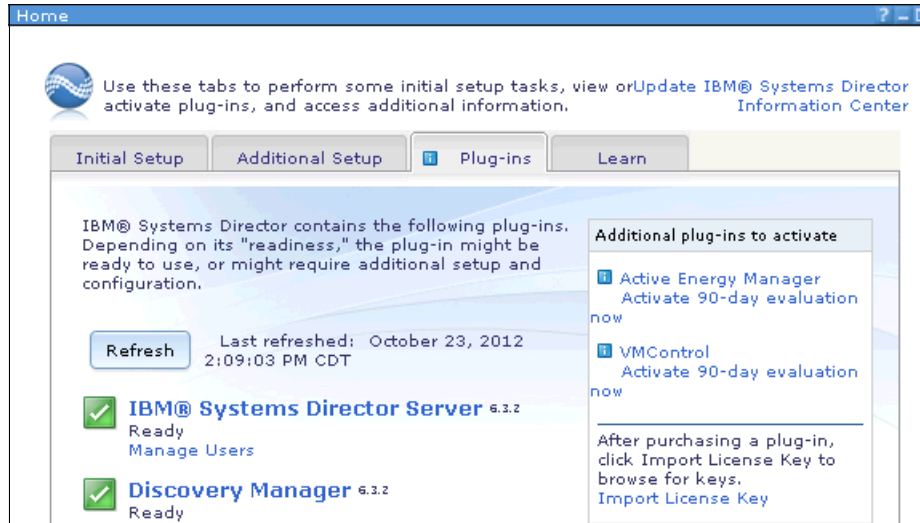


Figure 1-61 UI license import

Figure 1-62 shows an example of importing the license key from the server installation code.

```
-bash-3.2# importkey ISD_express_edition_power.lpsa
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON
AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM,
LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE
ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT
AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE
TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN
"ACCEPT" BUTTON, OR USE THE PROGRAM; AND

- PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND
PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, or "99" to go back to the previous screen.
1
Importing license keys.
IBM Systems Director Express Edition
All keys imported successfully.
```

Figure 1-62 CLI license import

For more information about the license, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.editions.doc%2Feditions_power_express_license.html

1.7 Installing on a Linux on Power platform

Useful information about the process of installing Systems Director on a Linux on Power platform is described. For the installation of Systems Director on Linux on Power, see the information center:

http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.director.install.helps.doc/fqm0_t_installing.html

1.7.1 Downloading the software

The Systems Director Management server code can be sourced from the following URL:

<http://www-03.ibm.com/systems/software/director/downloads/mgmtservers.html>

Place the code on the Linux on Power system by using a file transfer method of your choice. After the code is on the Linux system, extract the installation files:

```
tar -zxf express_Power_Linux_Director_base.tar.gz
```

1.7.2 Prerequisites

To determine whether the Linux distribution fulfills the software requirements, change to the `/server/checkds` directory. Each Linux distribution that is supported has additional Red Hat Package Manager (RPMs) packages that need to be installed. Look for the `checkds.sh` script in the `checkds` folder. This script checks the state of the server and whether the server is supported for the Systems Director server. If all the required RPM packages are installed, look for a return code of 0.

The `checkds` script invokes a `/checkds/checklists/lin-server-chklist.properties` checklist file. This file is unique for each supported OS on which the Systems Director server is installed.

Before the installation of Systems Director on Linux on Power, review Table 1-4 on page 45. Use the links in the footnotes to source the additional required RPM packages.

Table 1-4 Software requirements for Linux on Power

Installation scenario	Required RPM packages on the Agent	Required RPM packages on the server
Red Hat Enterprise Linux Advanced Platform, version 5.x on IBM Power systems	<ul style="list-style-type: none"> ▶ compat-libstdc++-<version>.ppc.rpm^a ▶ servicelog-0.2.9-0.ppc64.rpm^b ▶ openssl097a-0.9.7a-9.<version>.ppc.rpm^c ▶ librtas-1.3.4-0.ppc64.rpm^b 	<ul style="list-style-type: none"> ▶ vacpp.rte^{d e} ▶ Required RPM packages on Agent
Red Hat Enterprise Linux Advanced Platform, version 6.* on IBM Power systems	<ul style="list-style-type: none"> ▶ compat-libstdc++-33.ppc^a ▶ libstdc++-4.4.4-13.el6.ppc.rpm^a ▶ pam-1.1.1-4.el6.ppc.rpm^a ▶ servicelog-1.1.7-2.el6.ppc64^a ▶ librtas-1.3.4-2.el6.ppc^a ▶ libservicelog-1.1.9-4.el6.ppc^a ▶ expat-2.0.1-9.1.el6.ppc^a ▶ compat-expat1-1.95.8-8.el6.ppc^a 	<ul style="list-style-type: none"> ▶ vacpp.rte^{d e} ▶ Required RPM packages on Agent
SUSE Linux Enterprise Server 10 on IBM Power Systems	<ul style="list-style-type: none"> ▶ compat-libstdc++-<version>.ppc.rpm^a ▶ libservicelog-1.1.9-1.ppc.rpm^b ▶ servicelog-1.1.7-1.ppc.rpm^b ▶ lsvpd-0.16.0-1.ppc.rpm^b ▶ librtas-1.3.5-1.ppc.rpm^b 	<ul style="list-style-type: none"> ▶ vacpp.rte^{d e} ▶ Required RPM packages on Agent
SUSE Linux Enterprise Server 11 on IBM Power Systems	<ul style="list-style-type: none"> ▶ libstdc++33-3.3.3-11.9.ppc64.rpm^a ▶ libservicelog-1.1.9-1.ppc.rpm^b ▶ servicelog-1.1.7-1.ppc.rpm^b ▶ lsvpd-0.16.0-1.ppc.rpm^b ▶ librtas-1.3.5-1.ppc.rpm^b ▶ pam-32bit-1.0.2-20.1.ppc64.rpm^a 	<ul style="list-style-type: none"> ▶ vacpp.rte^{d e} ▶ Required RPM packages on Agent ▶ gcc-4.3-62.198.ppc64.rpm ▶ gcc-c++-4.3-62.198.ppc64.rpm ▶ libstdc++43-devel-4.3.3_20081022-11.18.ppc64.rpm ▶ gcc43-c++-4.3.3_20081022-11.18.ppc64.rpm ▶ glibc-devel-2.11.1-0.17.4.ppc64.rpm ▶ linux-kernel-headers-2.6.32-1.4.13.noarch.rpm
SUSE Linux Enterprise Server 11 SP2 on IBM Power Systems	<ul style="list-style-type: none"> ▶ libstdc++33-3.3.3-11.9.ppc64.rpm^a ▶ libservicelog-1.1.9-1.ppc.rpm^b ▶ servicelog-1.1.7-1.ppc.rpm^b ▶ lsvpd-0.16.0-1.ppc.rpm^b ▶ librtas-32bit-1.3.6-010.1.ppc64.rpm^a ▶ ppc64-diag-2.4.2-0.14.12.ppc64.rpm^a ▶ libvdp2-2.1.3-0.9.1.ppc64.rpm^a ▶ pam-32bit-1.0.2-20.1.ppc64.rpm^a ▶ pam-modules-32bit-11-1.22.1.ppc64.rpm^a 	

- a. Obtain this RPM package from the operating system distribution media. There might be minor version variations from the versions that are listed, which is acceptable.
- b. Obtain this RPM package from IBM Service and productivity tools for Linux on Power Systems at <https://www14.software.ibm.com/webapp/set2/sas/f/1opdiags/home.html>. Select your Linux distribution and then select the appropriate tab for your version. Follow any special instructions for each RPM package. For RHEL5, if the listed rpm version is not available on the website, get it from the RHEL4 tab.
- c. Obtain this RPM package from the operating system distribution media in addition to openssl 0.9.8, which is installed by default.
- d. Server only.
- e. Obtain the tar.gz package from <https://www-304.ibm.com/support/docview.wss?uid=swg24030460>. Untar and install the three included RPM packages. This action applies for all platforms.

32-bit and 64-bit RPM packages: 64-bit RPM package file names include ppc64. 32-bit RPM package file names include ppc. If the listed RPM package shows ppc, you need the 32-bit version. The platform agent does not install if you show the 64-bit version only.

For software requirements, see this website:

<http://www.ibm.com/developerworks/wikis/display/WikiPtype/Software+requirements+for+Director+6.3+on+Linux+on+Power>

Run the **checks.sh** script (Figure 1-63). Check for the return code 0. If the return code is not 0, review, fix, and run again.

```
[root@xs-2120rhelppc checksd]# ./checks.sh
Java: /root/ISD632/server/checkds/jvm/plinux/bin/java
Starting IBM Systems Director Pre-Installation Utility...
Finished analysing system
Creating reports...
Install Readiness Text report being written to
/tmp/checkds/reports/checkDS_Text_20121022_134508.txt
Install Readiness Error Text report being written to
/tmp/checkds/reports/checkDS_Error.txt
Install Readiness Detailed HTML report being written to
/tmp/checkds/reports/checkDS_Detailed_20121022_134509.html
Install Readiness Summary HTML report being written to
/tmp/checkds/reports/checkDS_Summary_20121022_134510.html
Unable to launch the default browser, please view the text or summary HTML report
manually.
Overall Report Return Code: 0
```

Figure 1-63 Running the checks script

1.7.3 Installing the Systems Director server

After you see the return code 0 from the `checkds` script (Figure 1-63 on page 46), proceed with the installation (Figure 1-64).

```
[root@xs-2120rhelppc server]# ./dirinstall.server
Agree to product license?
[1-Agree|0-Disagree]:1
..../....
Enter 1 to use the Agent Manager installed with this server (recommended)
Enter 0 to use an existing Agent Manager (advanced) : 1
Enter Resource Manager username : isd4itso
Enter Resource Manager password :
Re-Enter Resource Manager password :
Enter Agent Registration password :
Re-Enter Agent Registration password :
[Add] [Element]: AgentManagerUserID [Value]: isd4itso
[Add] [Element]: AgentManagerPassword [Value]:
{aes:3C5SnKQL63SjkEy44Gs+vHF6nQzC+Dil1NzNvSiAzzk=}fFn7zXZpwvsH3wYuP1yCIw==
[Add] [Element]: ManagerRegistrationPassword [Value]:
{aes:3C5SnKQL63SjkEy44Gs+vHF6nQzC+Dil1NzNvSiAzzk=}fFn7zXZpwvsH3wYuP1yCIw==
DataSourceConfig.sh=0
DataStoreInstall.sh=0
GenerateCertificates.sh=0
EncryptAMPProps.sh=0
WebConfig.sh=0
usmi-cas-setup.sh=0
Installation of the IBM Systems Director Server 6.3.2 succeeded.
To start the server manually, run /opt/ibm/director/bin/smstart.
To see the status, run /opt/ibm/director/bin/smstatus [-r].
```

Figure 1-64 Summary output of `dirinstall.server`

After the installation completes successfully, start Systems Director on Linux on Power (Figure 1-65).

```
[root@xs-2120rhelppc server]# /opt/ibm/director/bin/smstart
Starting IBM Director...The starting process may take a while. Please use smstatus to
check if the server is active.
[root@xs-2120rhelppc server]# /opt/ibm/director/bin/smstatus -r
Starting
Active
```

Figure 1-65 Starting Systems Director on Linux on Power

After the Systems Director server returns an Active status (Figure 1-65 on page 47), go to the Login panel (Figure 1-66).



Figure 1-66 IBM Systems Director login panel

After you log in, select the **Plug-ins** tab and select **IBM Systems Director Server** to see an overview of the server and associated properties (Figure 1-67).

Management Server

IBM® Systems Director Server

Manage the IBM® Systems Director server. View the server status and properties. Also view users, and the roles they have been assigned.

IBM® Systems Director Status

System: xs-2120rhelppc.itso.ral.ibm.com

Status: ■ OK (last restart: 12/3/12 1:28 AM)

2 Systems discovered

Authentication type:
Known ports in-use: 41700, 8421, 9513, 8422, 9511, 9512, All possible ports

Trace and error logs: /opt/ibm/director/lwi/logs

Database:
DB2/LINUXPPC64 SQL09076
IBM Data Server Driver for JDBC and SQLJ 4.14.88

Server:
5.5% CPU % Utilization
15,572 Memory Usage
8.9% Storage used
1 Active users

Common tasks

- System discovery
- View and collect inventory
- Find a task
- Find a resource
- Resource Explorer

Figure 1-67 IBM Systems Director Server



Fundamentals

Preferred practices and tips for are described for the three basic functions of IBM Systems Director 6.3: Discovery, Inventory, and Updates.

The following topics are described:

- ▶ 2.1, “Discovery” on page 52
- ▶ 2.2, “Endpoint management” on page 59
- ▶ 2.3, “Firewall ports” on page 59
- ▶ 2.4, “Inventory” on page 64
- ▶ 2.5, “Updates” on page 82

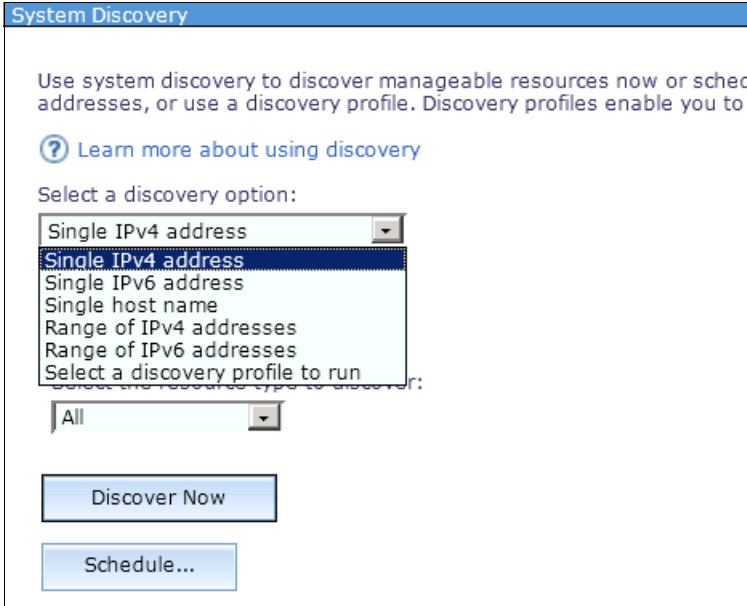
2.1 Discovery

Systems Director 6.3 can discover various types of endpoints. For multiple discovery options and multiple resource types to discover, see the Discovery section of the web interface.

For additional information about the discovery and inventory processes of Systems Director, see the Systems Director Discovery Information Center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.discovery.helps.doc%2Ffqm0_t_discovering_and_inventorying_resources.html

Figure 2-1 displays the available options to specify the endpoints that need to be discovered. You can limit the discovery process to a single address or range of sequential addresses. Or, you can use a discovery profile.



The screenshot shows a web interface titled "System Discovery". It contains the following elements:

- A header bar with the text "System Discovery".
- Introductory text: "Use system discovery to discover manageable resources now or schedule discovery at a later time. You can specify IP addresses, or use a discovery profile. Discovery profiles enable you to discover resources of a specific type or range of addresses."
- A link: "? Learn more about using discovery".
- A label: "Select a discovery option:".
- A dropdown menu with the following options:
 - Single IPv4 address (highlighted)
 - Single IPv6 address
 - Single host name
 - Range of IPv4 addresses
 - Range of IPv6 addresses
 - Select a discovery profile to run
- A label: "Select the resource type to discover:".
- A dropdown menu with the option "All".
- Two buttons: "Discover Now" and "Schedule...".

Figure 2-1 Discovery options

Figure 2-2 shows the resource options that are available to discover. Use resource types to limit the discovery process to protocols that are based on the resource type to discover.

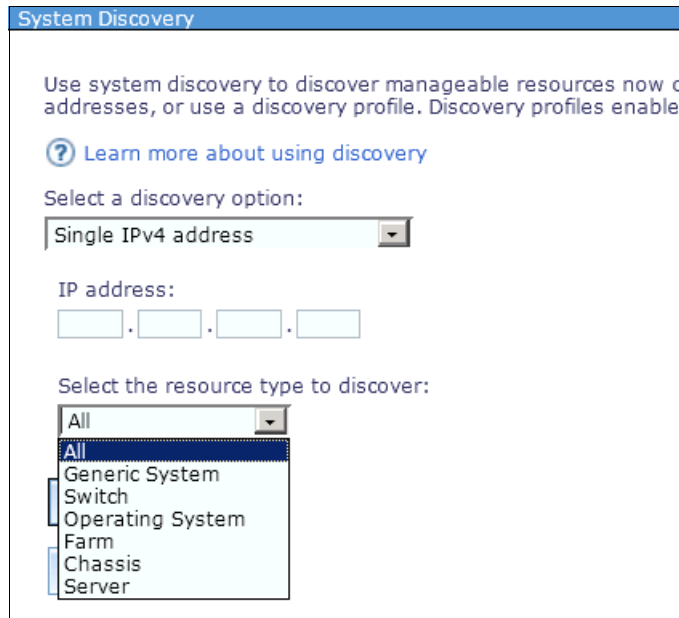


Figure 2-2 Resource options

Follow these guidelines to use the discovery task efficiently:

- ▶ Discover only the systems that you intend to manage.
Limiting discoveries to systems that you intend to manage speeds up the discovery process. You eliminate discovering other devices that might support the discovery protocols.
- ▶ Keep the IP address ranges as small as possible.
Limiting the number of addresses in a single request can improve the reliability of the discovery.
- ▶ Specify the types of resources to discover (avoid the use of All).
Systems Director can skip discovery protocols that are inappropriate for your resources. Skipping inappropriate discovery protocols results in shorter discovery time.
- ▶ Schedule the discovery of large numbers of systems during off-hours.
Scheduling large discovery jobs off-hours improves the reliability of the discovery process and helps with the additional network traffic.
- ▶ Where possible, use Discovery Profiles and specify individual IP addresses or use Service Location Protocol (SLP) Directory Agents.
Making the profile as specific as possible minimizes discovery time because Systems Director runs only the protocols that are configured.
SLP Directory Agents reduce network traffic and increase discovery speed.

2.1.1 Discovery profiles

Using discovery profiles is the best way to efficiently and effectively perform a discovery within Systems Director. Figure 2-3 displays the Advanced Tasks section, which gives you the options to manage discovery profiles.

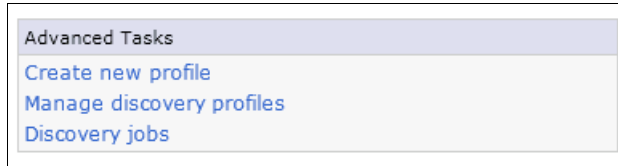


Figure 2-3 Advanced Tasks page

Figure 2-4 shows an example of creating a discovery profile for a BladeCenter chassis.

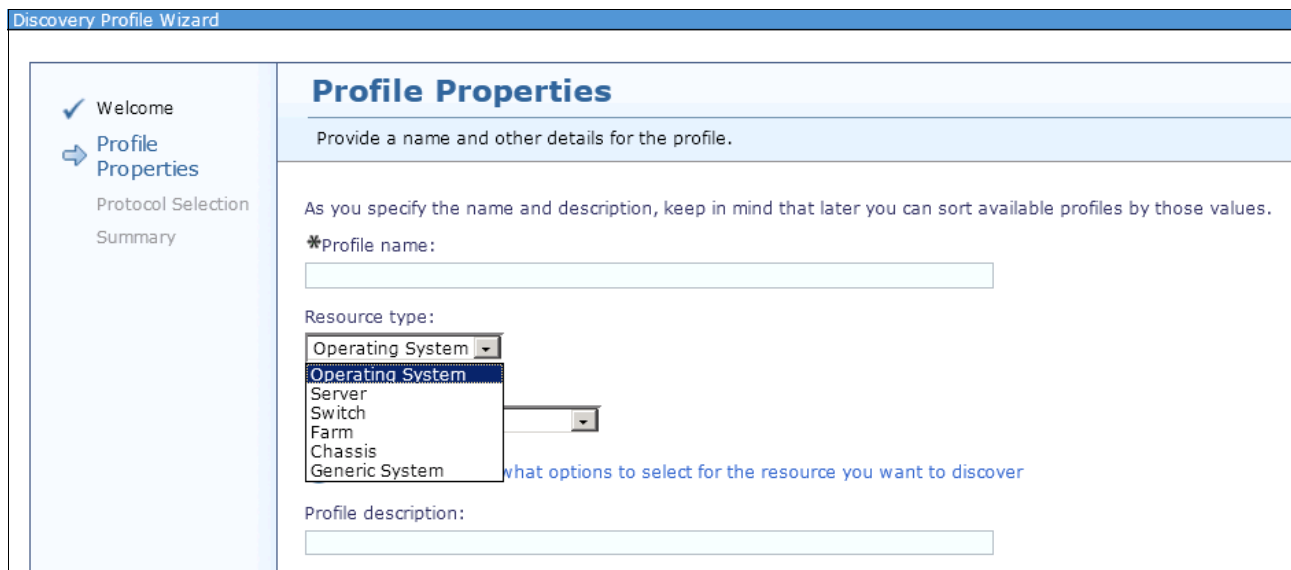


Figure 2-4 Profile Properties page

Figure 2-5 is the Protocol Selection page. If the chosen resource type supports additional discovery protocols, the protocols are listed.

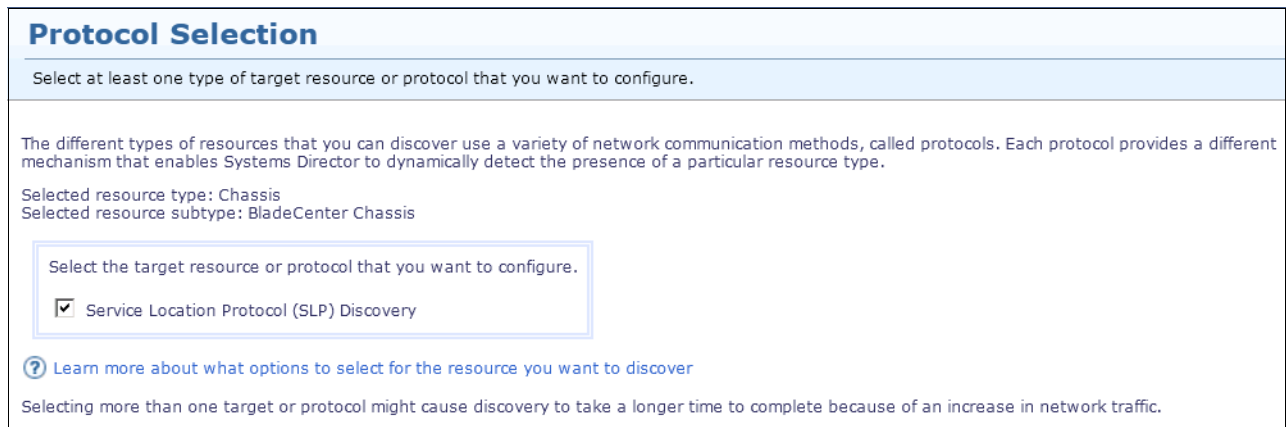


Figure 2-5 Protocol Selection page

Figure 2-6 shows where you configure how to discover your endpoints. Depending on the network, Unicast, Multicast, and Broadcast can be used. For best results, the use of Unicast is advised. With this option, you can specify an IP address or sequential range of IP addresses of endpoints. You also can import a group of nonsequential IP addresses by importing a text file or a CSV file that contains one IP address per line.

Service Location Protocol (SLP) Configuration

Configure settings for SLP discovery.

Specify how to configure SLP discovery.
You can use either unicast or multicast and broadcast to perform this discovery. You can also configure Service Location Protocol (SLP) directory agents.

Use this section to configure unicast or multicast and broadcast.
[? Learn more about unicast, multicast, and broadcast](#)

Choose a mechanism for discovering systems based on IP address:

Unicast

Select how to specify the IP addresses that you want to discover: [? Learn more about importing IP addresses](#)

Add a single IP address

Single IP address or beginning range:

Ending range:

IP addresses:

Multicast / Broadcast

Enable multicast

Enable general broadcast

Use this section if you want to configure Service Location Protocol (SLP) discovery agents.
 Configure SLP directory agents [? Learn more about configuring SLP directory agents](#)

Figure 2-6 SLP Configuration page

In Figure 2-7, you can enter credentials that automatically request access to the endpoint after the discovery.

Access Request

Configure settings to automatically request access to discovered systems.

You can specify to automatically request access to a resource after it is discovered.
Note: When discovering storage, always automatically request access.

Request access later

Use the following user ID and password

User ID:

Password:

Automatically requesting access might significantly increase the time required to perform discovery.

Figure 2-7 Access Request page

Figure 2-8 displays the new Discovery Profile wizard summary.

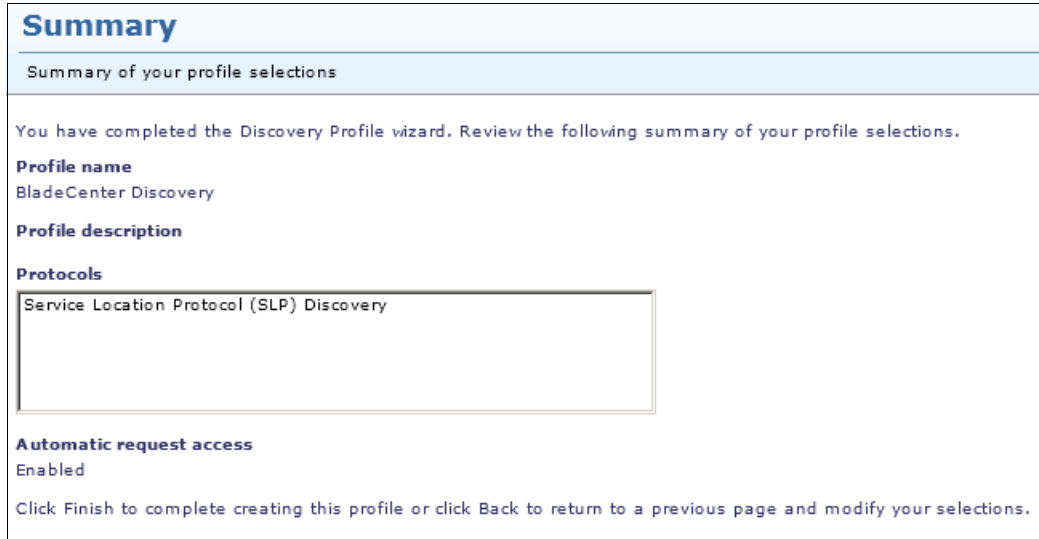


Figure 2-8 Summary

Figure 2-9 displays how to choose the profile that you created, which can be run immediately or scheduled.

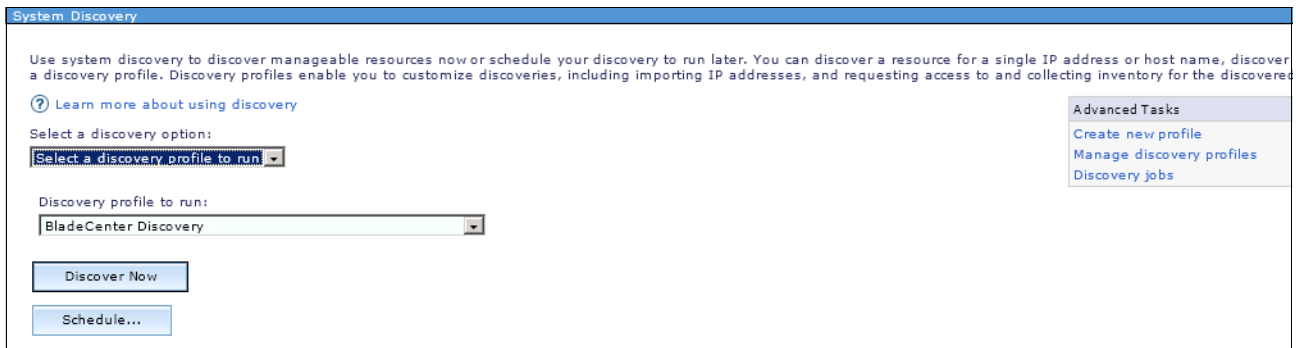


Figure 2-9 Selecting a discovery profile

2.1.2 BladeCenter discovery

To successfully discover a BladeCenter Advanced Management Module (AMM), you must set several AMM prerequisites:

- ▶ Increase TCP Command Mode protocol to at least 10 connections.

Systems Director needs several concurrent connections to successfully communicate with a BladeCenter AMM.

Figure 2-10 shows the AMM page where the TCP Command Mode Protocol is listed.

The screenshot displays the AMM (Advanced Management Module) configuration page for a server bay. The left sidebar shows a navigation menu with 'Network Protocols' highlighted. The main content area is divided into three sections:

- TCP Command Mode Protocol**:
 - Command mode: 10 connections
 - Secure command mode: 0 connections
 - Command mode inactivity timeout: 600 seconds
- Service Location Protocol (SLP)**:
 - SLP: Enabled
 - Address type: Multicast
 - Multicast address: 239.255.255.253
- File Transfer Protocol (FTP)**:
 - FTP server: Enabled
 - FTP idle timeout (seconds): 300

Figure 2-10 TCP Command Mode Protocol page

- ▶ Enable SNMPv1 and SNMPv3. Set the trap destination to the IP address of the Systems Director server. Set the Access Type to **Get** or greater.

By enabling SNMPv1 and SNMPv3, Systems Director uses the connection to collect a more comprehensive inventory. Figure 2-11 shows the AMM SNMPv1 and SNMPv3 setting page. Both the AMM SNMPv1 and SNMPv3 agents need to be enabled.

Simple Network Management Protocol (SNMP)

SNMP traps* Enabled

* If you enabled SNMP traps, you must also define an alert recipient from the [Alerts](#) page, and one

SNMPv1 agent† Enabled

† If you enabled the SNMPv1 agent, you must also define at least one community below.

Community Name	Access Type	Fully Qualified Hostnames or IP Addresses‡
ISD	Set	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
<input type="text"/>	Get	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
<input type="text"/>	Get	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>

‡ The value 0.0.0.0 is not a valid trap destination IP address, so it is ignored for sending traps. One trap destination IP address.

SNMPv3 agent§ Enabled

Figure 2-11 SNMP configuration

- ▶ SNMPv3 needs a user profile that is associated to it. Set the Access type to **Set** (Figure 2-12).

The user profile that is associated to SNMPv3 is used when you request access from the AMM.

SNMPv3 User Profile 6

Context name: context6

Authentication protocol: None

Privacy protocol: None

Privacy password:

Confirm privacy password:

Access type: Set

Fully qualified hostname/IP address for traps:

Figure 2-12 SNMPv3 User Profile page

Tip: Reboot AMM after these changes.

2.2 Endpoint management

Systems Director has multiple methods to manage different endpoints. The method depends on the type of equipment that you plan to manage. Servers are the most common endpoints.

Complete these prerequisites to manage endpoints by using System Director:

- ▶ Verify that the Domain Name System (DNS) functions correctly for both forward and reverse lookup.

Systems Director uses standard networking technologies, such as DNS, to identify and communicate with the endpoints.

- ▶ Open the necessary firewall ports.

Systems Director uses several ports to communicate with various endpoints that need to be open. Each type of device requires a group of ports. Determining which ports to open depends on what you plan to manage.

For more information, see this information center page:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.plan.helps.doc%2Ffqm0_r_all_available_ports.html

- ▶ Determine how you want to manage your systems, either agentless, Platform Agent, or Common Agent:
 - Agentless management provides “hardware alerting” out-of-band either through the Integrated Management Module (IMM) or AMM. With agentless management, you can inventory your systems by using distributed component object model (DCOM) for Windows or Secure Shell (SSH) for Linux.

For more information about agentless systems, see this information center page:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.install.helps.doc%2Ffqm0_t_preparing_agentless_managed_systems.html

- Platform Agent is the lightweight agent that is installed on Windows or Linux systems that provides everything that agentless management provides. Platform Agent also provides comprehensive hardware alerts from the OS level.

For more information about Platform Agent systems, see this information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.main.helps.doc%2Ffqm0_c_platform_agent.html

- Common Agent uses more resources from the system. Common Agent provides everything that the Platform agent offers. Common Agent can interact and monitor the operating system performance, services, and processes.

For more information about Common Agent systems, see this information center page:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.main.helps.doc%2Ffqm0_c_common_agent.html

2.3 Firewall ports

Table 2-1 on page 60 through Table 2-18 on page 64 list the TCP and User Datagram Protocol (UDP) ports that need to be open for specific Systems Director functions to work correctly.

Table 2-1 BladeCenter AMM (out-of-band)

Protocol	Description	Integrated System Development (ISD) server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
TCP Command Mode	Ongoing communication/ management	6090, TCP Outbound	6090, TCP Inbound
UDP	Native events	13991, UDP Inbound	13991, UDP Outbound
Simple Network Management Protocol (SNMP)	SNMP communication/traps	162, TCP, UDP Inbound Outbound	162, TCP, UDP Inbound Outbound
Trivial File Transfer Protocol (TFTP)/SNMPv3	Updating AMM firmware	69, UDP, Inbound 121, UDP Inbound Outbound	69, UDP Outbound 121, UDP Outbound Inbound

Table 2-2 IMM1/IMM2 (out-of-band rack servers)

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
UDP	Native events	13991, UDP Inbound	13991, UDP Outbound

Table 2-3 Management module (MM), remote supervisor adapter 1/2

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
CIM	Ongoing communication/ management	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)
TFTP	Updates for System x/Flex servers that run ESXi	69, UDP Outbound	69, UDP Inbound

Table 2-4 Flex Chassis Management Module (CMM)

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
CIM	Ongoing communication/management	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)
SFTP	Update CMM firmware	9520, TCP Outbound	9520, TCP Inbound

Table 2-5 Hardware Management Console (HMC)

Protocol	Description	ISD server port	Managed endpoint port
SSH	Ongoing communication with limited management	22, TCP Outbound	22, TCP Inbound
CIM	Ongoing communication/management	5989, TCP Inbound Outbound (secure)	5989, TCP Inbound Outbound (secure)

Table 2-6 Windows agentless

Protocol	Description	ISD server port	Managed endpoint port
DCOM	Ongoing communication with limited management	135, TCP, UDP Outbound (software installation) 137 - 139, TCP, UDP Outbound 445, TCP, UDP Outbound	135, TCP, UDP Inbound (software installation) 137 - 139, TCP, UDP Inbound 445, TCP, UDP Inbound

Table 2-7 Linux agentless

Protocol	Description	ISD server port	Managed endpoint port
SSH	Ongoing communication with limited management	22, TCP Outbound	22, TCP Inbound

Table 2-8 AIX agentless

Protocol	Description	ISD server port	Managed endpoint port
SSH	Ongoing communication with limited management	22, TCP Outbound	22, TCP Inbound

Table 2-9 VMWare ESXi

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
CIM	Ongoing communication/ management	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)

Table 2-10 ISD Platform Agent

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	427, TCP, UDP Inbound Outbound	427, TCP, UDP Inbound Outbound
CIM	Ongoing communication/management	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)	5988, TCP Inbound Outbound (unsecure) 5989, TCP Inbound Outbound (secure)

Table 2-11 ISD Common Agent (CAS)

Protocol	Description	ISD server port	Managed endpoint port
SLP	Discovery	14252, TCP, UDP Inbound Outbound	14252, TCP, UDP Inbound Outbound
CAS	All ongoing communication/ management	9510, TCP Inbound Outbound 9511 - 9513, TCP Inbound 20000, TCP Inbound	9510, TCP Inbound 9511 - 9513, TCP Outbound 20000, TCP Outbound

Table 2-12 I/O modules

Protocol	Description	ISD server port	Managed endpoint port
SSH	Ongoing communication with limited management	22, TCP Outbound	22, TCP Inbound
SNMP	Monitoring	162, TCP, UDP Inbound Outbound	162, TCP, UDP Inbound Outbound
TFTP/SFTP/FTP	Firmware updates	FTP 20 - 21 TCP Inbound SFTP 9520 TCP Inbound TFTP 69 UDP Inbound	FTP 20 - 21 TCP Outbound SFTP 9520 TCP Outbound TFTP 69 UDP Outbound

Table 2-13 SNMP Devices

Protocol	Description	ISD server port	Managed endpoint port
SNMP	SNMP communication/traps	162, TCP, UDP Inbound Outbound	162, TCP, UDP Inbound Outbound

Table 2-14 ISD Server Service and Support Manager

Protocol	Description	ISD server port	Managed endpoint port
HTTPS	Communication with IBM	443, TCP Outbound	N/A
FTPS	Service log upload	21, TCP Outbound	N/A

Table 2-15 ISD Server Update Manager

Protocol	Description	ISD server port	Managed endpoint port
HTTP	Check for updates Download updates	80, TCP, Outbound	N/A
HTTPS	Check for updates Download updates	443, TCP, Outbound	N/A

Table 2-16 ISD Server web interface

Protocol	Description	ISD server port	Managed endpoint port
HTTP	HTTP communication with ISD web interface (auto redirects to HTTPS)	8421, TCP, Inbound	N/A
HTTPS	HTTPS communication with ISD web interface	8422, TCP, Inbound	N/A

Table 2-17 Default Managed DB2 database on ISD server

Protocol	Description	ISD server port	Managed endpoint port
FCM	Database communication	50010, TCP Inbound Outbound	N/A

Table 2-18 ISD cli (smcli)

Protocol	Description	ISD server port	Managed endpoint port
TCP	Command-line interface (CLI)	2044, TCP Inbound Outbound	N/A

2.4 Inventory

Inventory is one of the most important tasks. Inventory needs to be run on all systems that are managed by the Systems Director server. Inventory information provides the basis for much of the functionality in Systems Director.

The following examples are good examples of functionality that depends on Inventory:

- ▶ Update Manager
- ▶ Compliance checks
- ▶ Dynamic groups

Inventory data for systems that are managed by Systems Director is stored in a database that is created and controlled by Systems Director. Since version 6.3, the default database format is IBM DB2.

Optionally, you can use external databases, such as IBM DB2, Oracle, and Microsoft SQL Server (the latter is for Windows platforms only). It is a preferred practice to use the built-in (local) IBM DB2 database, which is created and controlled by Systems Director at installation.

When a system is discovered by the Systems Director, a basic inventory scan runs for this system. This scan includes IP address, host name, OS, and if an agent is installed, the agent version. For additional information beyond these properties, the Systems Director needs full authorized access to the system.

When a system has access, run an inventory scan for this system to collect the complete inventory information. The complete inventory information includes hardware, software, and driver information from the system.

The following topics are described:

- ▶ 2.4.1, “Inventory data and collection profiles” on page 64
- ▶ 2.4.2, “Collecting inventory” on page 71
- ▶ 2.4.3, “Viewing inventory” on page 75
- ▶ 2.4.4, “Exporting inventory” on page 78

2.4.1 Inventory data and collection profiles

Systems Director uses inventory collection profiles to collect inventory data from discovered resources.

Systems Director uses profiles to manage the inventory collection tasks that you create and run. An *inventory collection profile* is a group of settings that are saved on the Systems Director server. The settings indicate the type of resources that are collected during the collection process.

By default, Systems Director includes the following inventory collection profiles:

- ▶ All Inventory

This profile collects inventory from all resources and encompasses all the other inventory collection profiles.

All inventory: The All Inventory profile is required if you intend to use Update Manager.

- ▶ All Hardware Inventory

This profile collects inventory from physical and virtual devices.

- ▶ All Software Inventory

This profile collects inventory from software resources.

- ▶ Basic System Information

This profile collects inventory from system resources.

These predefined inventory profiles are read-only and cannot be deleted or edited. However, you can use these existing profiles to create your own profiles.

The use of inventory discovery profiles provides a predefined template to collect the inventory information that you need. This template is useful when you want to use the inventory information that Systems Director collects from the system for asset tools. Or, this template is useful if you need specific information from the system without going through all of the available inventory information.

To create your own inventory discovery profile, follow these steps:

1. Start on the View and Collect inventory page. Select **Manage Profiles** next to the profile selection (Figure 2-13).

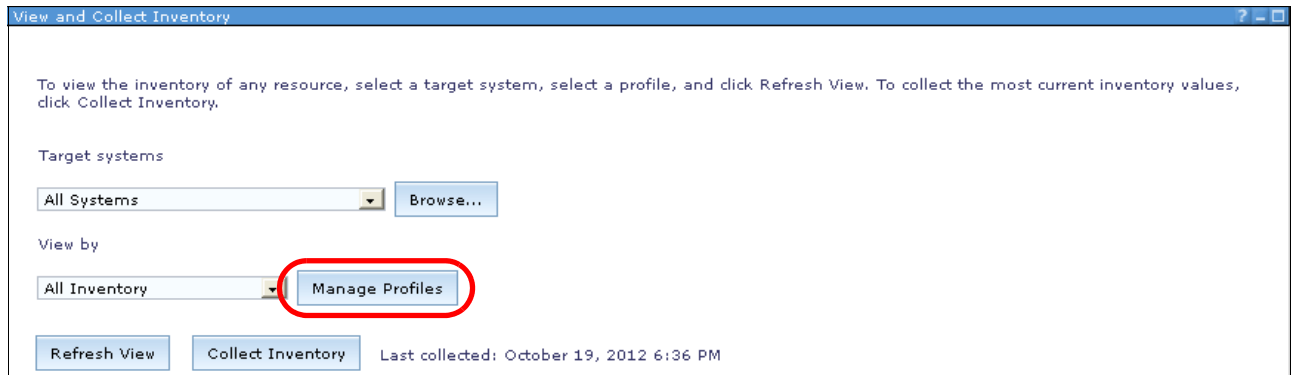


Figure 2-13 Manage inventory discovery profiles

2. Select either to create a profile or copy an existing profile. When a function is selected, the Create Inventory Profile wizard opens. In our example, we create a profile. The first window is the Welcome page (Figure 2-14). Click **Next** at the bottom of the page (not shown) to continue.

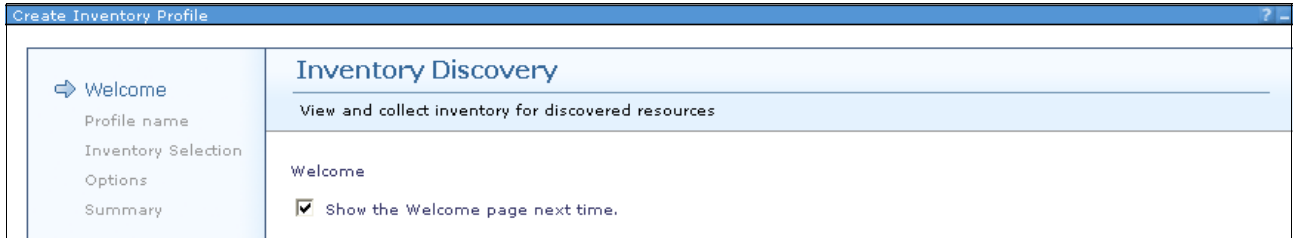


Figure 2-14 Inventory Discovery Profile wizard - Welcome panel

3. In Figure 2-15, give your profile a name. If you chose to copy an existing profile, the default name is copy_of_profilename. In our example, we name the profile book as shown in Figure 2-15. A description is optional. Click **Next** to continue.

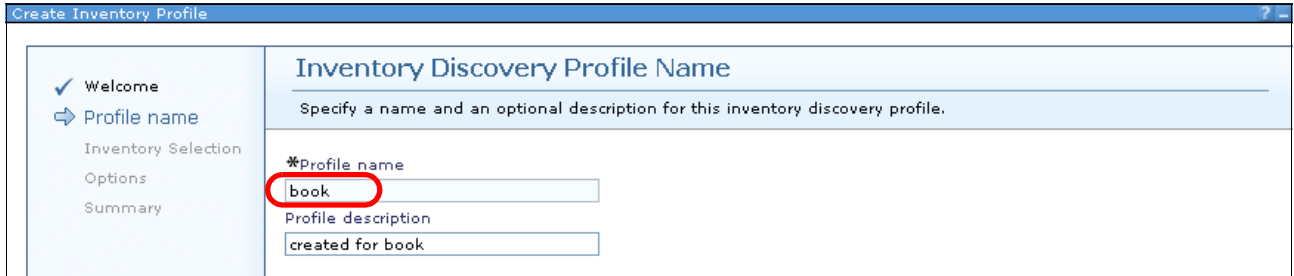


Figure 2-15 Inventory Discovery Profile wizard profile name

4. In Figure 2-16, select which inventory resources to collect with your profile. To select an inventory resource, expand the resource groups on the left, make your selection, and click **Add** to copy your selection to the selected resources. You cannot copy complete resource groups. Instead, you must select each resource in a resource group to select the complete group. Click **Next** to continue.

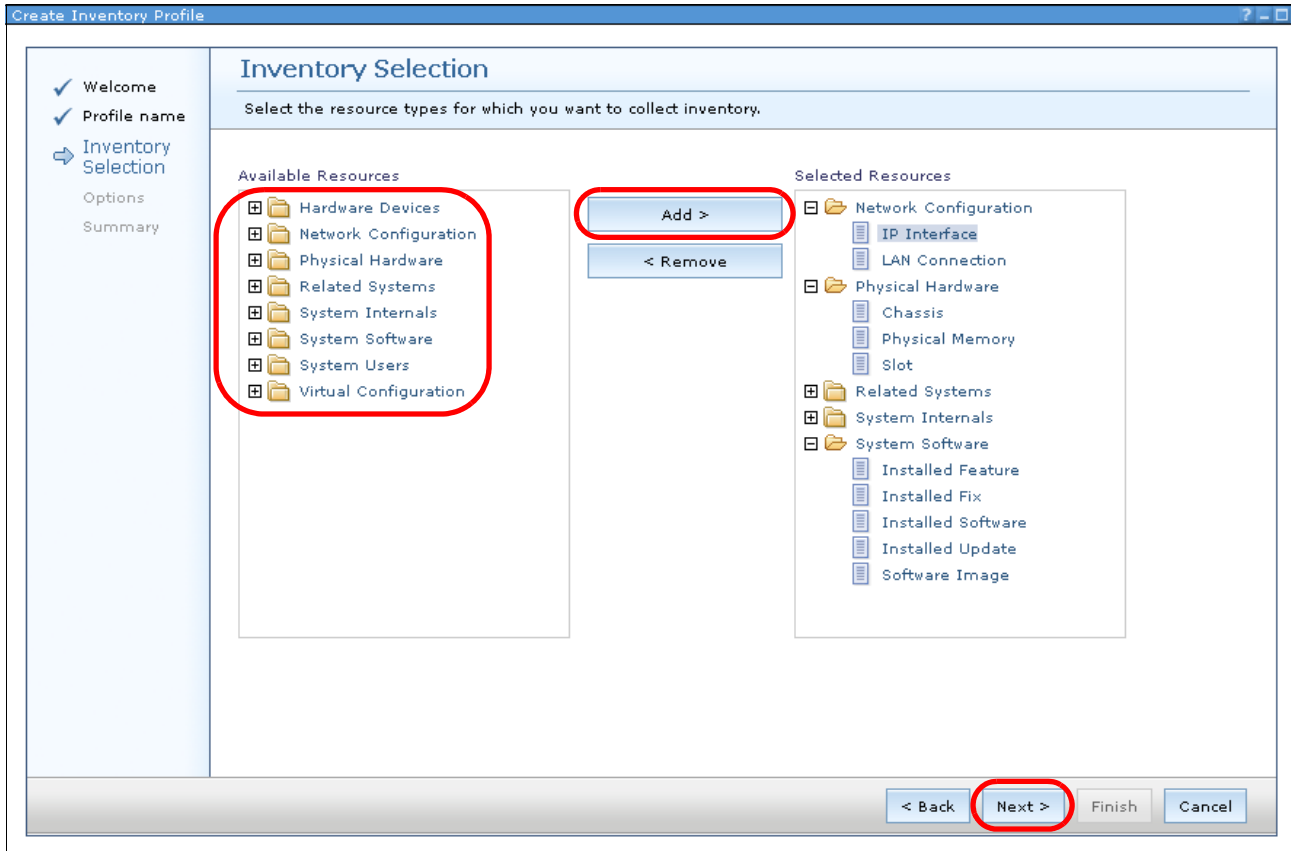


Figure 2-16 Inventory Discovery Profile wizard -Inventory Selection

5. In Figure 2-17, select the inventory service. You can either let the system select the inventory service or you can manually configure the discovery service.

If you select **Let the system choose**, click **Next** to see the option window as described in step 7 on page 70.

If you select **Let me manually configure the discovery services** and click **Next**, you see Figure 2-18. Go through the definition of the discovery services. In this window, you can select the available inventory profiles.

In most cases, letting the system choose the discovery service is easier. With this method, no configuration mismatches occur and you include all necessary functions.

In our example, to show the available functions of this wizard, we choose the manual configuration. In our example, only one discovery service available, the CIT Software Discovery module, which we select.

Select the modules (if more than one service is available) that you want to use and click **Next**.

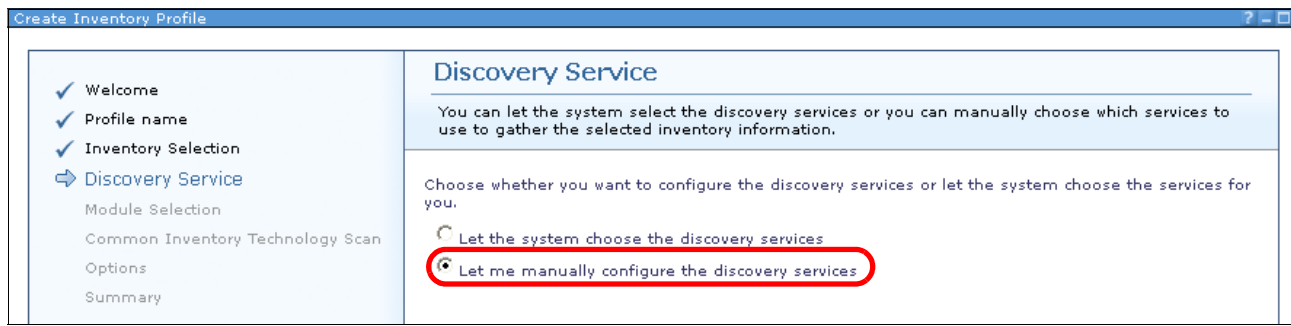


Figure 2-17 Select Discovery Service

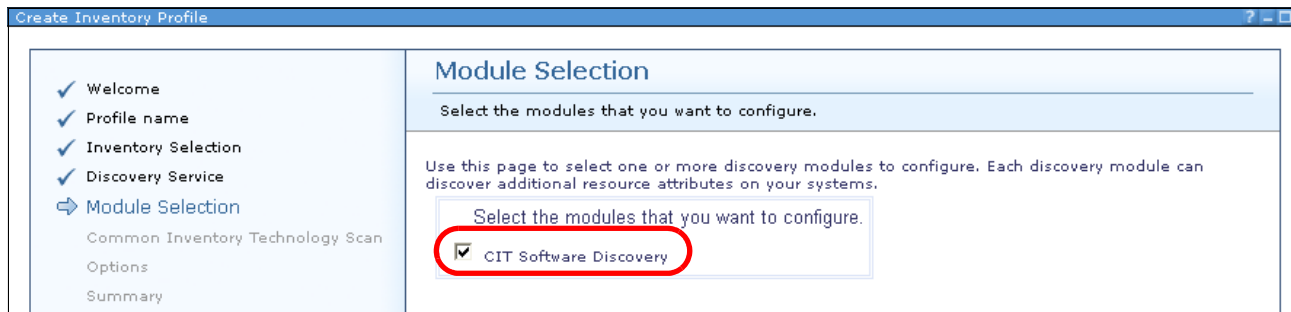


Figure 2-18 Module Selection

6. In our example, the option menu for the CIT Software Discovery module opens (Figure 2-20 on page 69). You can select whether you want to use the registry, the catalog, or both for the inventory collection. In our example, we select **Use both**.

If you select the registry, the registry information from the system is used to collect software inventory information. If you select the catalog, the internal software catalog is used to collect software inventory information. When you choose both options for the software inventory collection, the CIT Software discovery module checks the registry and the catalog to collect software information.

The default software signature file is the `softwaresignature.xml` file (Figure 2-19).

```
<!--  
Licensed Materials - Property of IBM  
(C) Copyright IBM Corp. 2010, 2011 All Rights Reserved  
US Government Users Restricted Rights - Use, duplicate or disclosure  
restricted by GSA ADP Schedule Contract with IBM Corp.  
-->  
<!-- IBM_COPYRIGHT_END -->
```

Figure 2-19 `softwaresignature.xml` file

If other modules are available, you see the option menus for these modules. Make your selection and click **Next**.

The screenshot shows a web-based configuration interface for 'CIT Software Discovery'. On the left is a navigation pane with a list of steps: Welcome, Profile name, Inventory Selection, Discovery Service, Module Selection, Common Inventory Technology Scan (highlighted with a blue arrow), Options, and Summary. The main content area is titled 'CIT Software Discovery' and contains the following text and controls:

- Use this page to select the type of common inventory technology scan to perform.
- Choose the common inventory technology option for the scan to use.
- Three radio button options: 'Use the registry', 'Use catalog', and 'Use both'. The 'Use both' option is selected and circled in red.
- A label 'Software Signature File' above a text input field containing the value 'softwaresignatures.xml'.

Figure 2-20 Options for CIT Software Discovery

7. In the Options panel, Figure 2-21, you can define the timeout period and the number of simultaneous collections.

Timeout period describes the length of time to wait for a response to inventory collection communications that are sent to systems. If the timeout value elapses before the response is received from the destination, no inventory data is collected from that target.

Maximum simultaneous collections describe the maximum number of agents from which the Systems Director server can simultaneously collect inventory. To help reduce network traffic, specify the lowest possible number of agents.

A check box asks whether you want to try failed agents again. If you select this function, Systems Director automatically tries again after failed collection attempts.

Click **Next** to continue.

The screenshot shows a software configuration window titled "Create Inventory Profile". On the left side, there is a vertical navigation pane with a list of steps: "Welcome", "Profile name", "Inventory Selection", "Discovery Service", "Module Selection", "Common Inventory Technology Scan", "Options" (which is highlighted with a blue arrow and a blue background), and "Summary". The main content area is titled "Options" and contains the instruction "Select a timeout period and a maximum number of simultaneous collections." Below this instruction, there are three configuration items: "Timeout period" with a dropdown menu set to "30" and the unit "Minutes"; "Maximum simultaneous collections" with a dropdown menu set to "5" and the unit "Agents"; and a checked checkbox labeled "Retry failed agents".

Figure 2-21 Options window

- The summary windows for the wizard open (Figure 2-22) where you can verify the settings that you entered. Click **Finish** at the bottom of the window (not shown) to save the Inventory Discovery profile that you created.

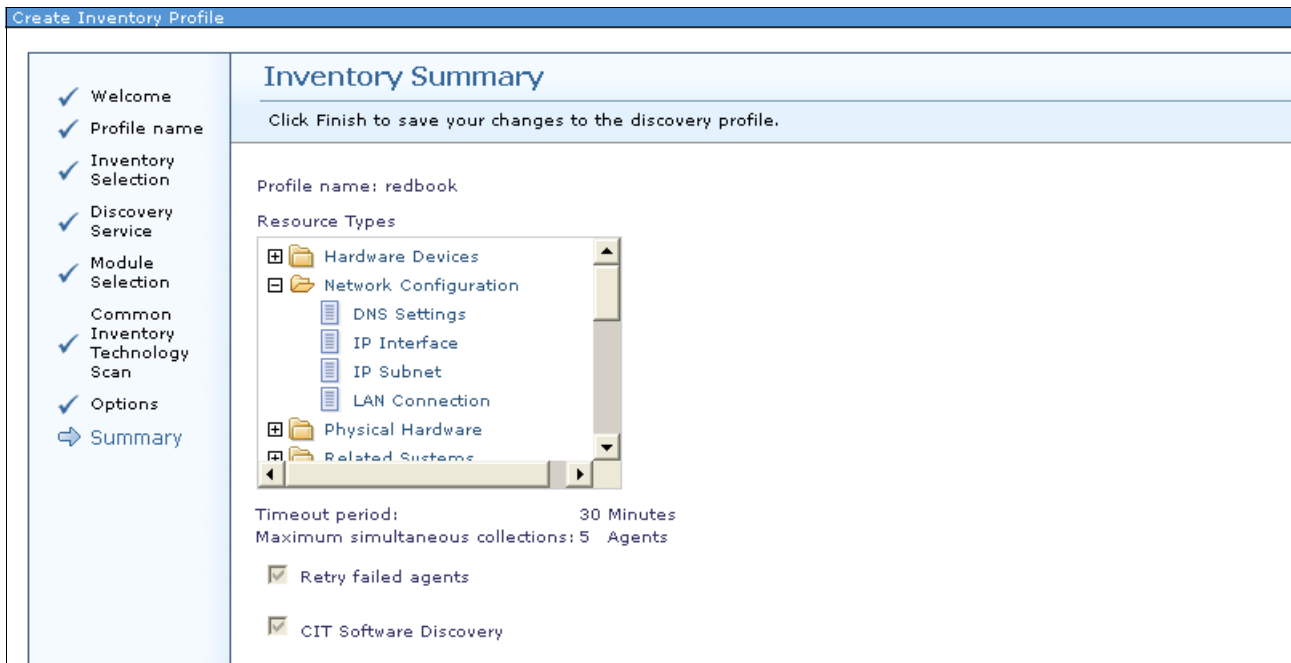


Figure 2-22 Summary view

- The list of available profiles for the inventory collection displays, including the profile that you created (Figure 2-23). In this window, you can edit or delete existing profiles.

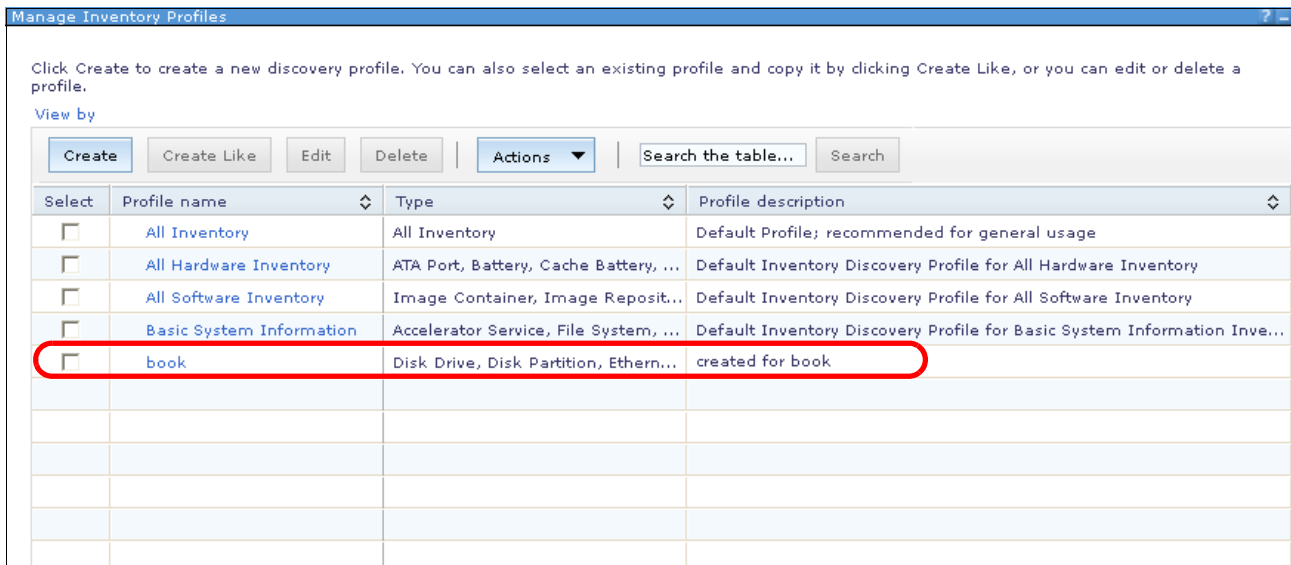


Figure 2-23 Inventory discovery profiles

2.4.2 Collecting inventory

Before you can view inventory for a resource, you must discover that resource by using discovery.

Inventory collection uses inventory collection profiles. You can use an existing profile to collect inventory for a system. If the inventory collection profile does not exist for inventory data type that you want to collect, first create the inventory collection profile. Ensure that the inventory collection profile contains the appropriate settings.

Follow these steps to perform an inventory collection:

1. Launch view and collect inventory. Systems Director offers you various ways to initiate this task:
 - On the home page, on the Initial Setup tab, click **Collect Inventory**, as shown in Figure 2-24.

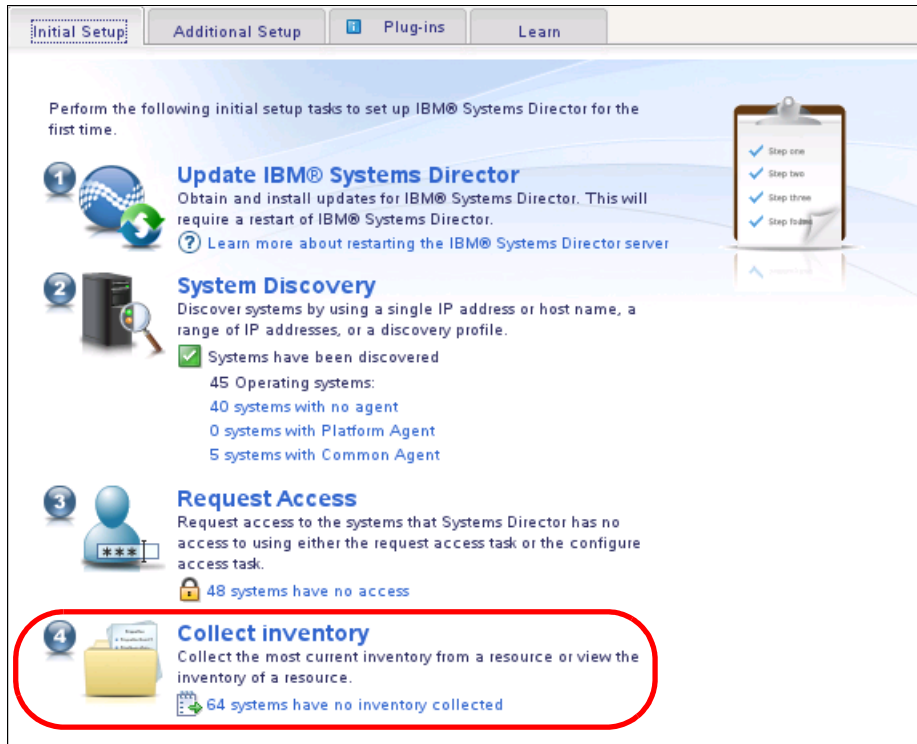


Figure 2-24 Inventory Collection from the Initial Setup tab

- On the leftmost tasks panel, click **Inventory** → **View and Collect Inventory**, as shown in Figure 2-25.



Figure 2-25 Select the View and Collect Inventory option from the left pane

- From the Systems Director Home page, click the **Plug-ins** tab and under Discovery Manager, click **View and Collect Inventory**, as shown in Figure 2-26.

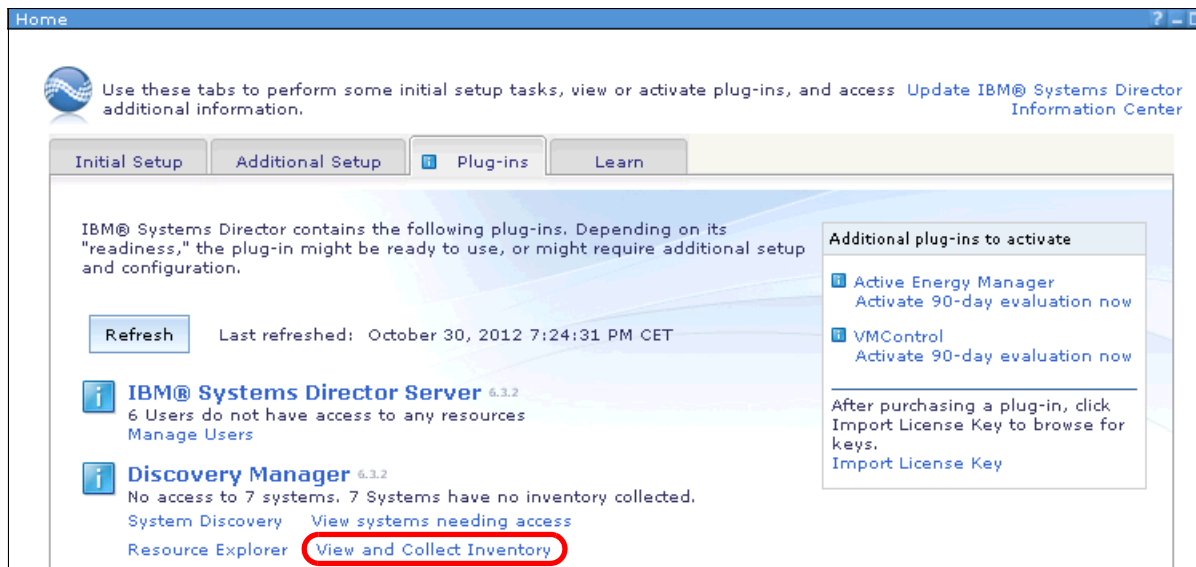


Figure 2-26 View and Collect Inventor from Home page

- In Resource Explorer, right-click a group or system. Then, from the menu, click **Inventory** → **View and Collect Inventory** (Figure 2-27).

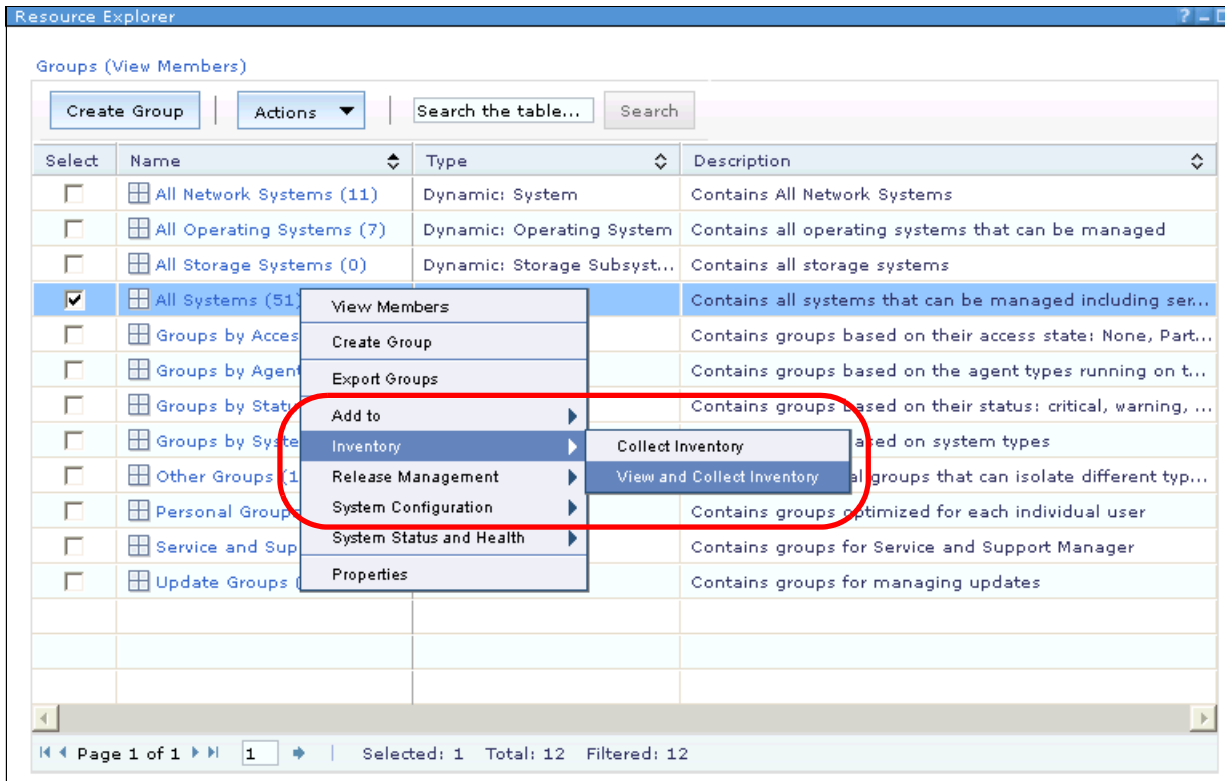


Figure 2-27 View and Collect Inventory from Resource Explorer

- The inventory task then launches (Figure 2-28). If not preselected, select the system or group for which you want to run the inventory collection. Then, you can select an Inventory Discovery profile. We describe how to create a profile in 2.4.1, “Inventory data and collection profiles” on page 64. Click **Collect Inventory** to start the process.

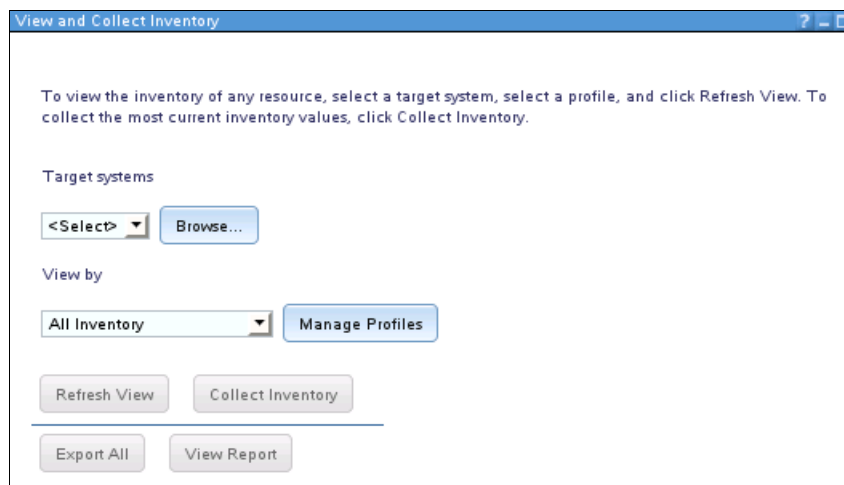


Figure 2-28 Inventory collection

3. A scheduler window opens (Figure 2-29). Select **Run Now** or specify a time to run the inventory collection.

The screenshot shows a 'Scheduler' dialog box with three tabs: 'Schedule', 'Notification', and 'Options'. The 'Schedule' tab is active. The 'Job name and schedule' section contains a text box with the job name 'Collect Inventory - November 1, 2012 12:22:47 PM EDT'. Below this, the instruction 'Choose when to run the job.' is followed by two radio buttons: 'Run Now' (unselected) and 'Schedule' (selected). The 'Schedule' section includes a '*Time:' field set to '12:22 AM' and a '*Date:' field set to 'Nov 1, 2012'. The 'Repeat Options' section shows a 'Frequency:' dropdown menu set to 'Weekly'. Below this, the instruction 'Run every week on the following days:' is followed by seven checkboxes: 'Sunday' (checked), 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday'. The 'Duration' section has three radio buttons: 'For', 'Until', and 'Unlimited' (selected). The 'Repeat forever' text is positioned to the right of the 'Until' radio button. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'. A red rounded rectangle highlights the 'Schedule' radio button, the time and date fields, the 'Repeat Options' section, and the day checkboxes.

Figure 2-29 Scheduler example for weekly, Sunday 12:22 a.m. setting

Schedule an inventory collection once a week. Schedule this inventory collection in off-hours so that the inventory collection does not affect your daily business. Also, run an inventory scan when you plan to update systems or install agents on the system.

4. After the schedule is defined or you select **Run Now**, click **OK**.
5. You can see the status of the task in the left pane under **Task Management** → **Active and Scheduled Task**.

2.4.3 Viewing inventory

After the inventory task completes, you can view the results. The following examples show different profiles.

Tip: When you select a single system, a summary shows at the top of the inventory information. If you select a group of systems, no summary is shown.

In our examples, we used the All Systems group to discover the inventory:

- ▶ Basic file system information (Figure 2-30)

Select	Name	System name	File System ...
<input type="checkbox"/>	/dev/loop0	SLES11	Unknown
<input type="checkbox"/>	/dev/sda2	SLES11	EXT3
<input type="checkbox"/>	/dev/sr0	SLES11	Unknown
<input type="checkbox"/>	udev	SLES11	Unknown

Figure 2-30 Basic systems information

- ▶ All software inventory (Figure 2-31)

Select	Name	System name	Version
<input type="checkbox"/>	3ddiag	SLES11	0.742-32.25
<input type="checkbox"/>	a2ps	SLES11	4.13-1326.33
<input type="checkbox"/>	aaa_base	SLES11	11-6.3
<input type="checkbox"/>	acli	SLES11	2.2.47-30.3
<input type="checkbox"/>	acpid	SLES11	1.0.6-91.6
<input type="checkbox"/>	agfa-fonts	SLES11	2003.03.19-156.21
<input type="checkbox"/>	alsasound	SLES11	1.0.18-16.3

Figure 2-31 All software information

- ▶ All hardware inventory (Figure 2-32)

Select	Name	System name	Model
<input type="checkbox"/>	BCM:44W4477-YK50200590ET	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590RK	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590U0	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590V4	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590V9	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590WA	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590WZ	IBM 7870AC1 06...	
<input type="checkbox"/>	BCM:44W4477-YK50200590XB	IBM 7870AC1 06...	
<input type="checkbox"/>	Chassis	SLES11	VMware Virtual
<input type="checkbox"/>	IBM:68Y8071-Y012UF06C01R	IBM 7870AC1 06...	
<input type="checkbox"/>	IBM:68Y8071-Y012UF06C01T	IBM 7870AC1 06...	

Figure 2-32 All hardware inventory

- ▶ All inventory (Figure 2-33)

Select	Name	System name	Capacity
<input type="checkbox"/>	L1 Cache	SLES11	16,3
<input type="checkbox"/>	L1 Cache	SLES11	16,3
<input type="checkbox"/>	L1 Cache	SLES11	16,3
<input type="checkbox"/>	L1 Cache	SLES11	16,3
<input type="checkbox"/>	L2 Cache	SLES11	524,2
<input type="checkbox"/>	L2 Cache	SLES11	524,2
<input type="checkbox"/>	L2 Cache	SLES11	524,2
<input type="checkbox"/>	L2 Cache	SLES11	524,2

Figure 2-33 All inventory

If you select a single system, a system summary shows at the top of the inventory information. This summary provides an overview of the system information:

- ▶ Operating system summary
- ▶ Network configuration summary
- ▶ Systems Director Agent version that is installed on the system
- ▶ Access state
- ▶ Supported protocols
- ▶ Firmware information

In Figure 2-34, we show a system that runs SLES11. The Systems Director server 6.3.2 is installed. The system runs on a virtual machine that is hosted by VMware ESXi.

The screenshot shows the 'Collected Items' sidebar on the left with 'Summary' highlighted. The main area displays the 'System Summary' for 'SLES11'. Below this are four summary tables: 'Software Summary', 'Network Summary', 'Asset Summary', and 'Utilization Summary'. At the bottom, there is an 'Installed Firmware' table with one entry for 'BIOS'.

System Summary	
System name:	SLES11
Type:	Operating System
Access State:	Full Access/Communication OK
Last Collected:	October 26, 2012 2:44 PM
Protocols:	SMIS, CAS, CIM, SSH

Software Summary	
Software Type:	Linux
Software Version:	11.0
Agent Version:	IBM-IBM Director Agent-v6.3.2, IBM-IBM Director Platform Agent-v6.3.2
System BIOS:	6.00

Network Summary	
Hostname:	SLES11
IP Addresses:	9.42.171.84
MAC Addresses:	000C2939F85C

Asset Summary	
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Machine Type:	VMware Virtual Platform
Serial Number:	VMware-56 4d 11 44 96 1 e 6b ac-25 f2 7c 50 c4 39 f8 5c
Architecture:	x86_64
UUID:	564d1144-961e-6bac-25f2-7c5 0c439f85c

Utilization Summary	
Number of Processors:	4
Number of Cores:	4
Max Processor Speed:	30000 MHz
Processor Family:	Unknown
Total Physical Memory:	24564964 KB
Free Physical Memory:	283444 KB

Installed Firmware					
Select	Name	System name	Category	Subcategory	V
<input type="checkbox"/>	BIOS	SLES11	BIOS	System	6

Figure 2-34 Inventory summary view (only available for a single system selection)

2.4.4 Exporting inventory

To use the inventory information outside the Systems Director, you can export the inventory information for a system or a group. This function might be useful to perform asset management tasks that are external to Systems Director. Or, this function can be useful if you want to print the inventory report for documentation.

Follow these steps to export the inventory data:

1. From the View and Collect Inventory page, click **Export All** (Figure 2-35).



Figure 2-35 Select Export All to export inventory data

2. Choose the format to which to export the inventory data (Figure 2-36). Various formats are available to export your data:
 - Hypertext Markup Language (HTML)
 - Extensible Markup Language (XML)
 - Comma Separated Variable (CSV)

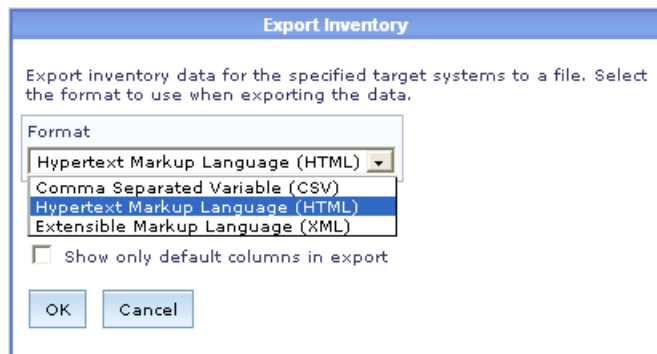


Figure 2-36 Select the format for export

3. After you select the format in which you want to export the inventory data, click **OK**.

If the HTML or XML format is selected, a web page that contains the data opens in your browser. You can save this data to a file or print the data, as needed. In our example, we use HTML as the file format (Figure 2-37).

Inventory Report SLES11

System name:	SLES11
Type:	Operating System
Access State:	Full Access/Communication OK
Last Collected:	October 26, 2012 2:44 PM
Protocols:	SMIS, CAS, CIM, SSH

Software Summary

Software Type:	Linux
Software Version:	11.0
Agent Version:	IBM-IBM Director Agent-v6.3.2, IBM-IBM Director Platform Agent-v6.3.2
System BIOS:	6.00

Network Summary

Hostname:	SLES11
IP Addresses:	9.42.171.84
MAC Addresses:	000C2939F85C

Asset S

Manufact
Model:
Machine
Serial N
Architect
UUID:

Utilization Summary

Number of Processors:	4
Number of Cores:	4
Max Processor Speed:	30000
Processor Family:	Unknown
Total Physical Memory:	24564964
Free Physical Memory:	283444

Hardware Devices

Cache Memory

Name	Capacity	Health State	Block Size	Volatile	Level	Read Policy	Write Policy	Changed Date	Consumab
L1 Cache	16384		1024					2012-10-26T14:44:21-04:00	16
L1 Cache	16384		1024					2012-10-26T14:44:21-04:00	16
L1 Cache	16384		1024					2012-10-26T14:44:21-04:00	16
L1 Cache	16384		1024					2012-10-26T14:44:21-04:00	16

Figure 2-37 HTML export

If the CSV format is selected, you can save or open the data with available applications as detected by your browser (Figure 2-38).

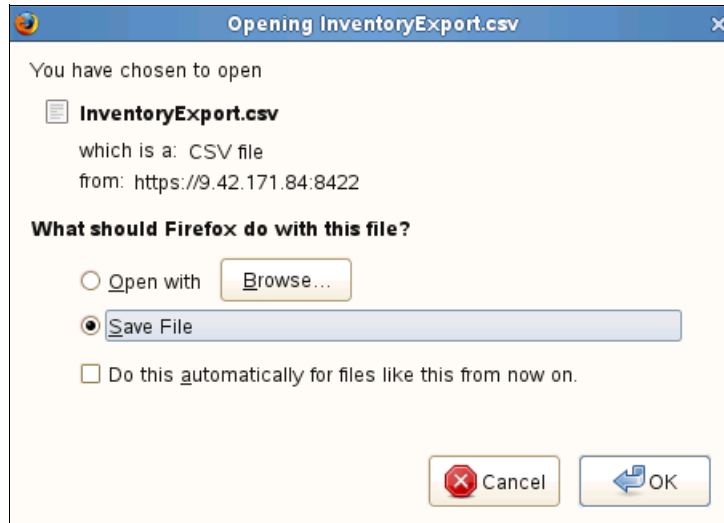


Figure 2-38 Save the CSV file

The CSV file can be used, for example, to import this data into an Excel worksheet (Figure 2-39).

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Cache Memory												
2	System na	Name	Capacity	Health Sta	Block Size	Volatile	Level	Read Polic	Write Polic	Changed C	Consumab	Created D	Free Spac
3	SLES11	L2 Cache	524288		1024					2012-10-26	0	2012-10-26	0
4	SLES11	L1 Cache	16384		1024					2012-10-26	16	2012-10-26	16384
5	SLES11	L1 Cache	16384		1024					2012-10-26	16	2012-10-26	16384
6	SLES11	L1 Cache	16384		1024					2012-10-26	16	2012-10-26	16384
7	SLES11	L2 Cache	524288		1024					2012-10-26	0	2012-10-26	0
8	SLES11	L2 Cache	524288		1024					2012-10-26	0	2012-10-26	0
9	SLES11	L2 Cache	524288		1024					2012-10-26	0	2012-10-26	0
10	SLES11	L1 Cache	16384		1024					2012-10-26	16	2012-10-26	16384
11													
12	Disk Partition												
13	System na	Name	Partition T	Partition S	Capacity	Free Spac	Bootable	Primary P	Block Size	Changed C	Created D	Health Sta	Number of
14	SLES11	/dev/sda1	Extended		2.15E+09				1024	2012-10-26	2012-10-26	OK	2104483
15	SLES11	/dev/sda2	Extended		1.05E+11				1024	2012-10-26	2012-10-26	OK	1.03E+08
16													
17	Ethernet Port												
18	System na	Name	Permanent	Speed	Port Numb	Enabled	Link Techn	Full Duplex	Auto Sens	Changed C	Created D	Maximum	Network A
19	SLES11	eth0	000C2939f	1000000		TRUE	Ethernet	TRUE	TRUE	2012-10-26	2012-10-26	10000	{ 00:0c:29
20													
21	Memory												
22	System na	Name	Capacity	Health Sta	Block Size	Volatile	Changed C	Created D	Ending Ad	Number of	Sequential	Starting Ad	State
23	SLES11	System M	2.52E+10	OK	1	TRUE	2012-10-26	2012-10-26	2.52E+10	2.52E+10	FALSE	0	Active
24													
25	Port Controller												
26	System na	Name	Controller T	State	Health Sta	Model	Manufactu	Protocol S	Changed C	Created D	Description		
27	SLES11	2f5301f4601f201f4501f5c0							2012-10-26	2012-10-26	Port Controller		
28	SLES11	eth0			OK				2012-10-26	2012-10-26	Port Controller		
29													
30	Processor												
31	System na	Name	Family	Maximum	Number of	Data Width	Model	Version	Address W	Changed C	Created D	Current Clk	State
32	SLES11	Unknown	Unknown	30000	1	32			32	2012-10-26	2012-10-26	1900	Started
33	SLES11	Unknown	Unknown	30000	1	32			32	2012-10-26	2012-10-26	1900	Started
34	SLES11	Unknown	Unknown	30000	1	32			32	2012-10-26	2012-10-26	1900	Started
35	SLES11	Unknown	Unknown	30000	1	32			32	2012-10-26	2012-10-26	1900	Started
36													
37	DNS Interface												
38	System na	Name	Host Name	Domain N	DNS Suffix	Append P	Append Pr	Changed C	Created D	Description			
39	SLES11	SLES11	SLES11					2012-10-26	2012-10-26	DNS Interface			
40													
41	IP Interface												
42	System na	Name	Dynamic #	IPv4 Addr	IPv6 Addr	Subnet M	Prefix Len	Gateway	Changed C	Created D	Network A	Description	
43	SLES11	9.42.171.8	FALSE	9.42.171.84		255.255.254.0			2012-10-26	2012-10-26	9.42.170.0	IP Interface	
44													
45	LAN Connection												
46	System na	Name	MAC Addr	Device Na	Network B	LAN ID	Aggregate	Aggr Cong	Changed C	Created D	Description		
47	SLES11	eth0	000C2939f	eth0	TRUE		FALSE		0	2012-10-26	2012-10-26	LAN Connection	

Figure 2-39 Imported inventory information into an Excel worksheet by using the CSV file

2.5 Updates

With Update Manager, a component of Systems Director, you keep the servers on your network at the software or firmware update levels that you want. Update Manager automatically checks for available updates and identifies which systems need attention. Update Manager also provides you with the ability to monitor your systems for needed updates. With Update Manager, you can schedule the updates at times that are convenient for you and your users.

Update Manager compares the update information that is loaded into it with the inventories of specified systems to determine whether updates are needed.

2.5.1 Prerequisites

Before you can start to use Update Manager to update your systems, ensure that an inventory of your system is performed. You can automate the collection of the inventory information as described in 2.4, “Inventory” on page 64.

To update your systems, the systems must be online and accessible. Therefore, you must have full access to the systems from the Systems Director server. The access state must be set to OK. Update Manager can be used to update agentless systems and systems with Platform Agent and Common Agent installed.

To update the BladeCenter AMM and server with Integrated Management Module I (IMMv1), you must configure a TFTP server. Systems Director includes a TFTP server. See 2.5.3, “Settings for Update Manager” on page 85.

The best way to check whether your system is up-to-date or needs an update is to use the Compliance Check function, which is described in 2.5.6, “Compliance check” on page 93.

2.5.2 What can be updated

The following list shows the supported updates and the systems to which updates can be applied. Unless otherwise noted, the systems can be agentless-managed systems, Common Agent-managed systems, and Platform Agent-managed systems.

The following list shows the supported updates and systems:

- ▶ Systems Director:
 - 6.3.x (Common Agent, Platform Agent, and the Systems Director server)
 - 6.2.x and 6.1.x (Common Agent and Platform Agent)
 - IBM Director V5.20.x (IBM Director Agent version 5.20 and IBM Director Core Services version 5.20)
- ▶ Technology levels (TLs) and service packs (SPs):
 - AIX 5.3 TL6 SP5 and later (the Systems Director server or Common Agent only)
 - AIX 6.1 (the Systems Director server or Common Agent only)
- ▶ SUSE Linux
- ▶ Red Hat Enterprise Linux
- ▶ Cumulative PTF packages and PTF groups for IBM i (formerly i5/OS™) 5.4 and later
- ▶ Hardware Management Console (HMC) systems at V7.3.3 SP2 or later
- ▶ Power Systems firmware for all systems that meet at least one of the following criteria:
 - Inband stand-alone (not managed by HMC or Integrated Virtualization Manager) Power Systems target systems that run AIX or Linux

Required: These systems must have the Common Agent installed.

- Out-of-band (managed by HMC) target systems

No Common Agent: No Common Agent is required in this case because SSH performs the update.

- Power Systems target systems that are managed by Integrated Virtualization Manager and that run Virtual I/O Server (VIOS) version 1.5.2.1 - Fix Pack (FP) 11.1 or later

No Common Agent: No Common Agent is required in this case because SSH performs the update.

- Migration, FPs, SPs, and interim fixes for VIOS version 1.5.2.1 - FP11.1 or later
- ▶ Device driver and firmware updates, or UpdateXpress System Pack updates, for System x servers that run Linux or Windows

Support is provided for servers that run all available agent and agentless levels. No support is available for updating IMM V2 systems that run IBM Director Agent 5.x.

- ▶ IBM BladeCenter I/O Module firmware
- ▶ IBM BladeCenter Management Modules, AMMs, and Pass-Thru Modules

Update Manager does not perform the following tasks:

- ▶ Installing new software products.
- ▶ Installing Systems Director agents on systems that currently do not have an agent.
Instead, install Systems Director agents with the Agent Manager plug-in of Systems Director.
- ▶ Migrating to any version of Systems Director from any version of IBM Director.
- ▶ Performing actions on systems that are not accessible.

You can perform update actions on those systems that are accessible only. To check whether the system is accessible, go to Resource Manager and check the access column. If there is a green circle icon, the access state is OK. If there is another icon (red, yellow, or gray), check the access state and return the system to the OK state.

- ▶ Uninstalling updates and rolling back updates are not supported.

Check several system-specific considerations before you use the Update Manager:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.updates.helps.doc%2Fqm0_c_um_platform_extensions.html

2.5.3 Settings for Update Manager

Before you start to use Update Manager, configure all of the necessary settings:

1. On the Update Manager page, click **Configure settings** as shown in Figure 2-40.

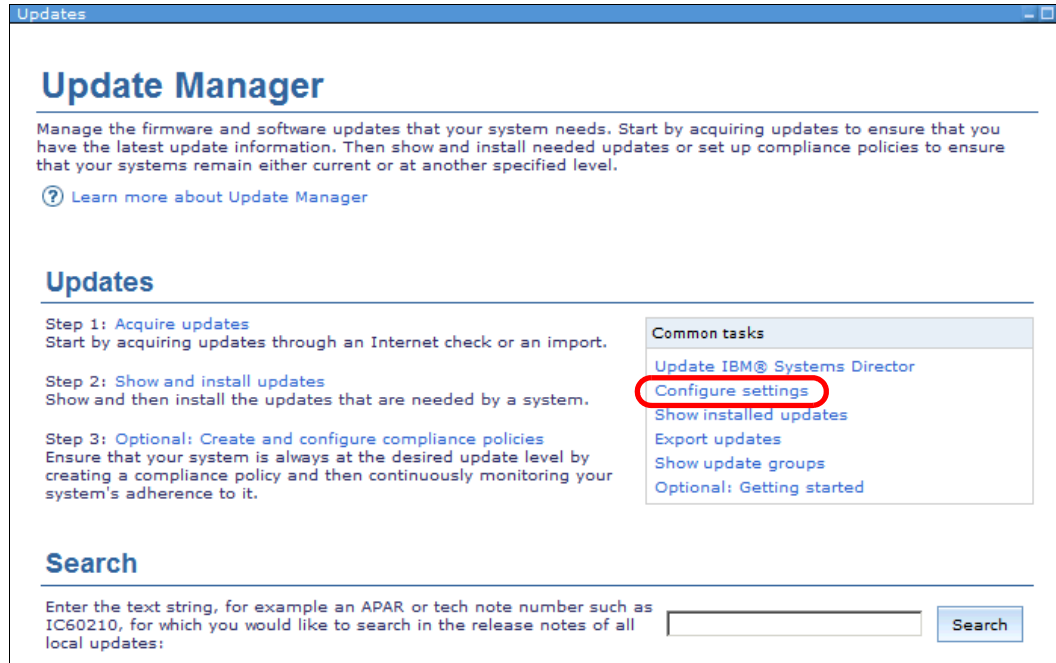


Figure 2-40 Update Manager: Configure settings

A new window opens. Adjust these settings:

- Connection to the Internet (if the Systems Director accessed the Internet)
 - Location for the local repository
 - Settings that are specific to System x and BladeCenter servers
 - Settings that are specific to AIX and VIOS systems
2. Select the **Connection** tab (Figure 2-41). You can configure a direct connection to the Internet or connect through an HTTP proxy server. After you make your selection, you can test the Internet connection by selecting **Test Internet Connection**.

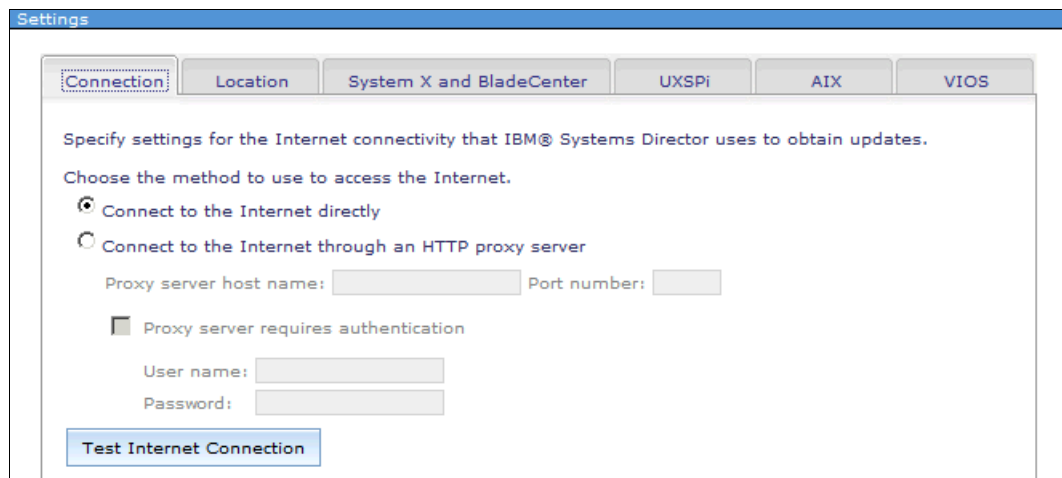


Figure 2-41 Connection tab

3. Select the **Location** tab (Figure 2-42). Define the size and location on disk of the local repository. The defaults are shown in Figure 2-42. The size might need to be increased. The size depends on the number of managed systems and the kinds of update packages that you want to deploy with the Systems Director server. The maximum size is 126 GB.

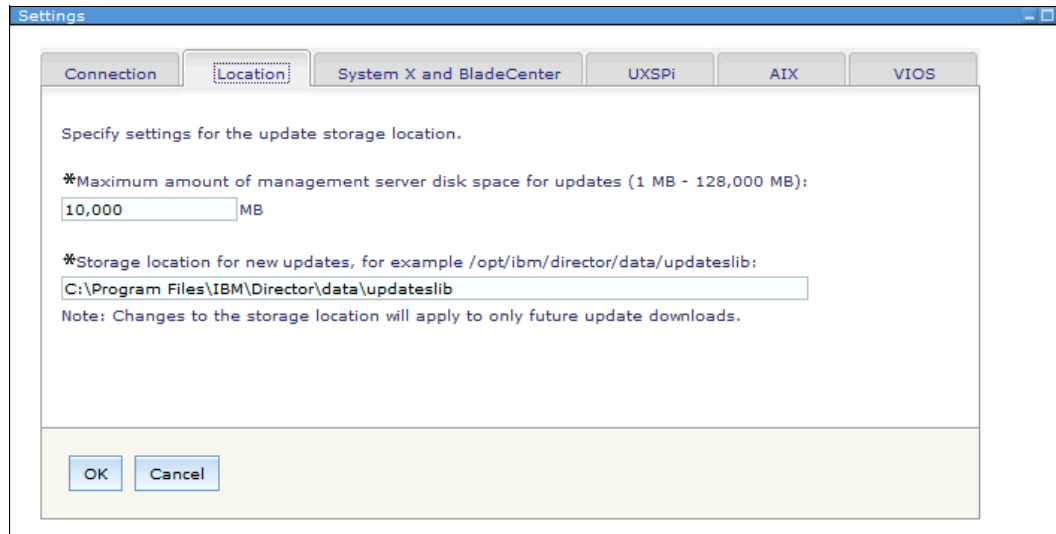


Figure 2-42 Location tab

4. In the System x and BladeCenter tab (Figure 2-43 on page 87), you can define the use of a TFTP or FTP server for updates. This definition is necessary for updating the AMM and also for updating systems with IMMv1.

For systems with IMMv2, this setting is not necessary. The service processor has enough internal memory to hold the update packages for updates to Unified Extensible Firmware Interface (UEFI), IMM, and preboot Dynamic System Analysis (pDSA).

The Systems Director server can be used as a TFTP server, as indicated in Figure 2-43. Therefore, you do not need to install an external TFTP or FTP server.

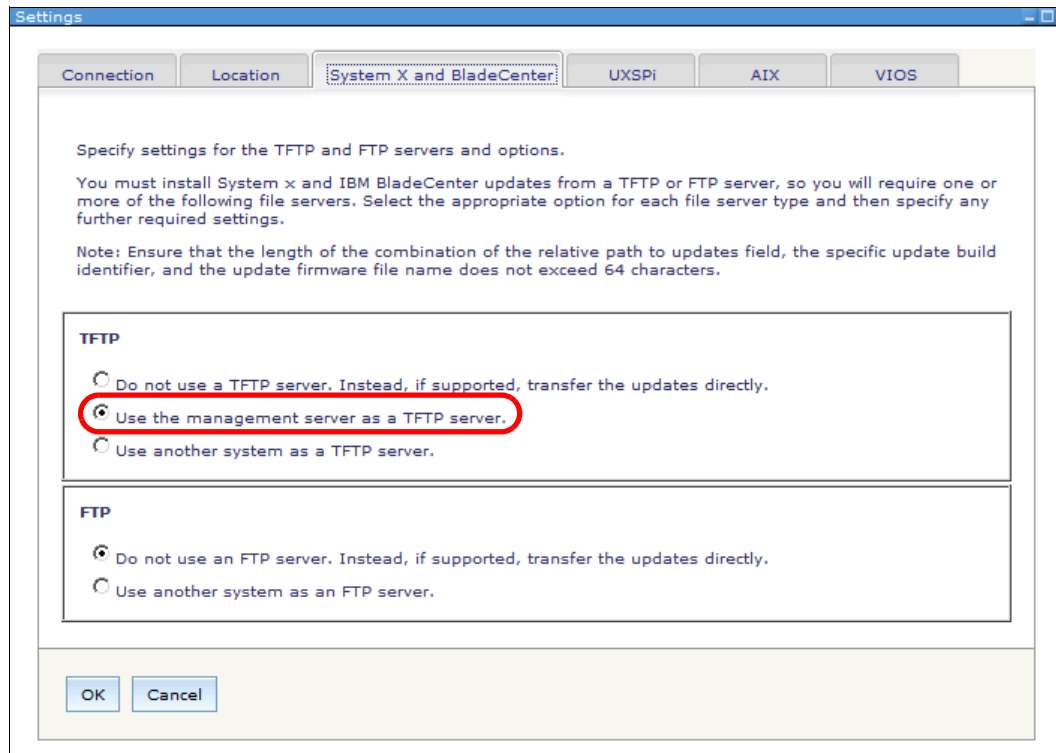


Figure 2-43 System x and BladeCenter: TFTP and FTP selection

5. The UXSPi tab, Figure 2-44, shows the installed UpdateXpress System Pack Installer (UXSPi) packages. Click **Import UXSPi** to import these packages to Systems Director to deploy them.

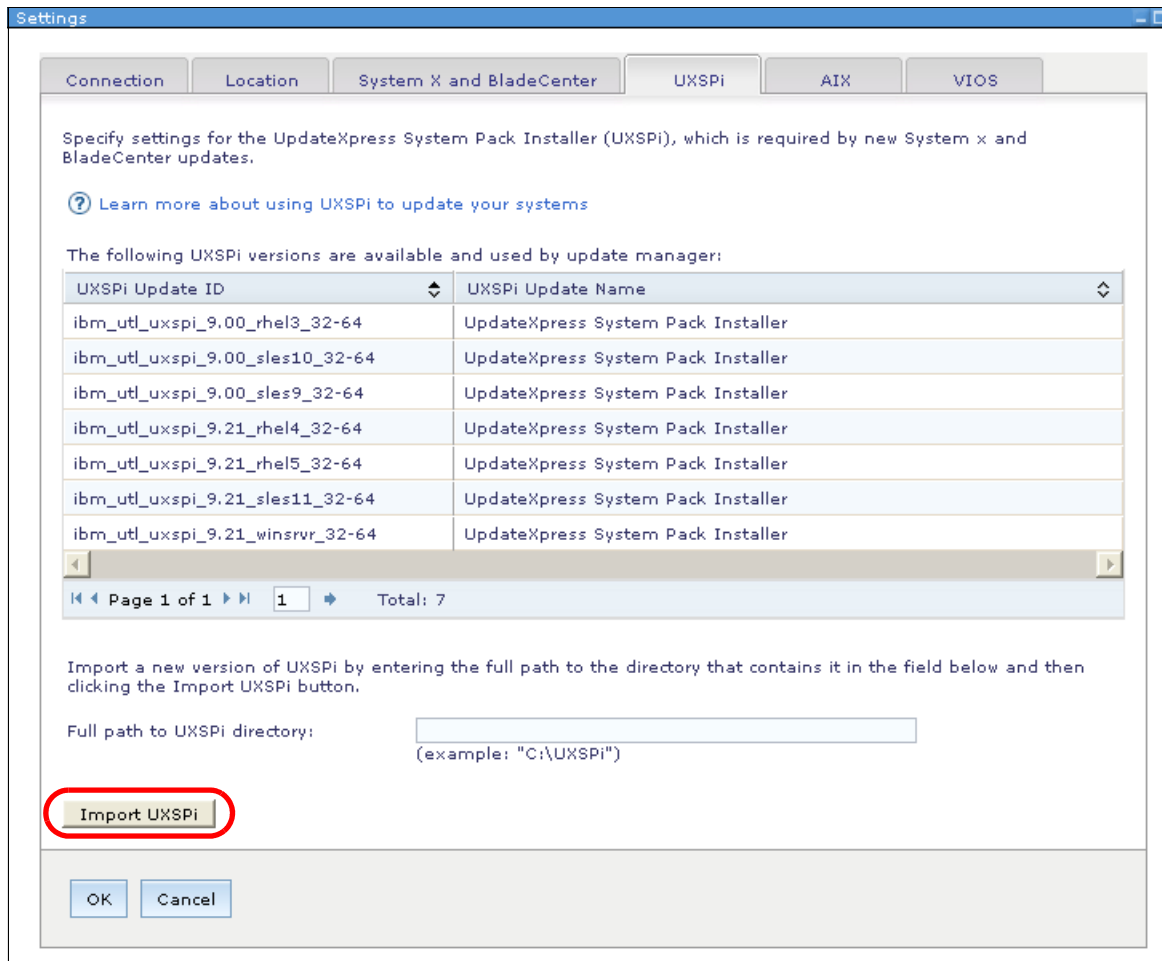


Figure 2-44 UXSPi: Show version or import UXSPi

To import the UXSPi packages, you need the Subsystem Device Driver (SDD) file for each package. If the file is missing, you are prompted that the file is needed before you can continue.

- The AIX tab (Figure 2-45) shows the selection for the AIX Network Installation Management (NIM) master. This NIM master is used for updates on AIX systems. Click **Browse** to select the AIX NIM master in your network.

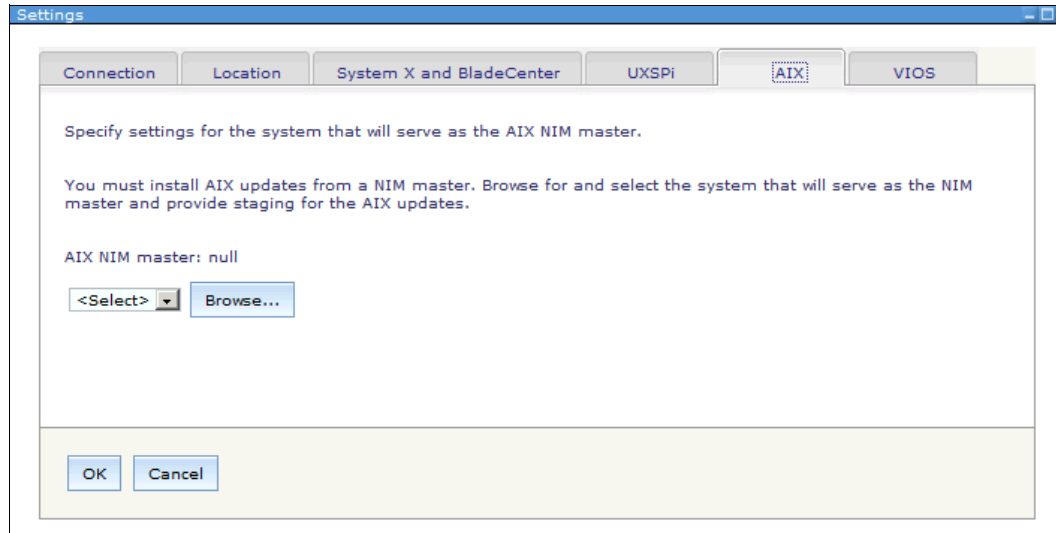


Figure 2-45 AIX: Define the AIX NIM master

- The VIOS tab (Figure 2-46) shows the selection for the VIOS NIM master. This VIOS NIM master is used for a VIOS upgrade (migration).

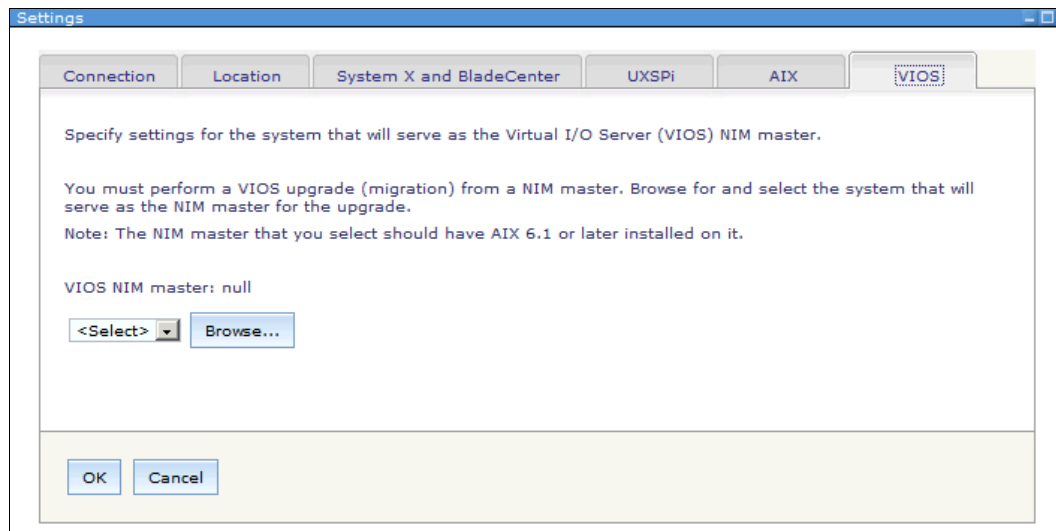


Figure 2-46 VIOS: Define the VIOS NIM master

2.5.4 Update Manager with Internet connection

When Systems Director connects to the Internet, use Update Manager to automatically check and download the update information from a central IBM repository. 2.5.3, “Settings for Update Manager” on page 85 describes setting up and verifying the Internet connection.

Perform these steps to retrieve updates directly from the Internet:

1. On the Update Manager home page, click **Acquire Updates** as shown in Figure 2-47.

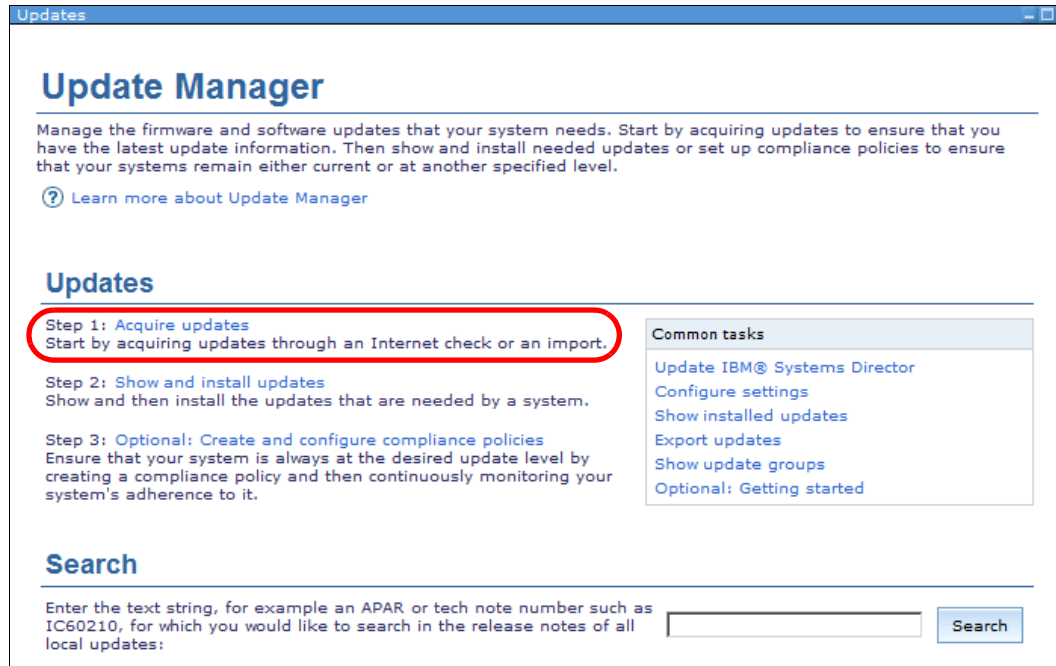


Figure 2-47 Update Manager: Acquire updates

2. In the Acquire Updates window (Figure 2-48), click **Check for Updates (Internet connection required)**.

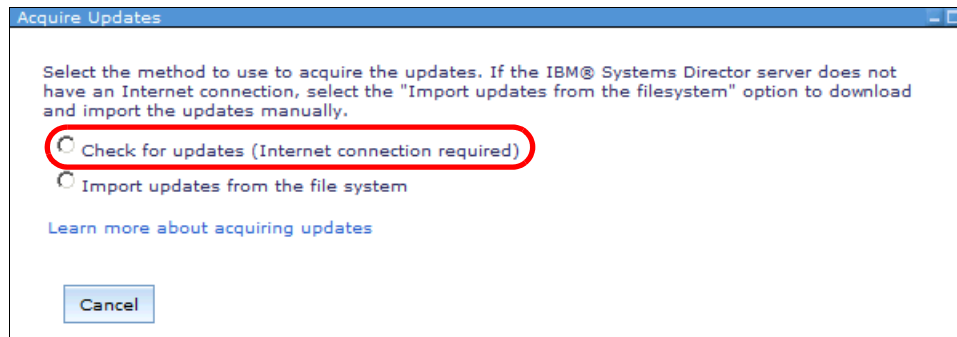


Figure 2-48 Selection for Internet or import

3. The window then expands as shown in Figure 2-49. A selection window opens where you select the update that the Update Manager looks for in the IBM repository.
4. Expand the Available update types on the left. Select the update types that you want and click **Add**.

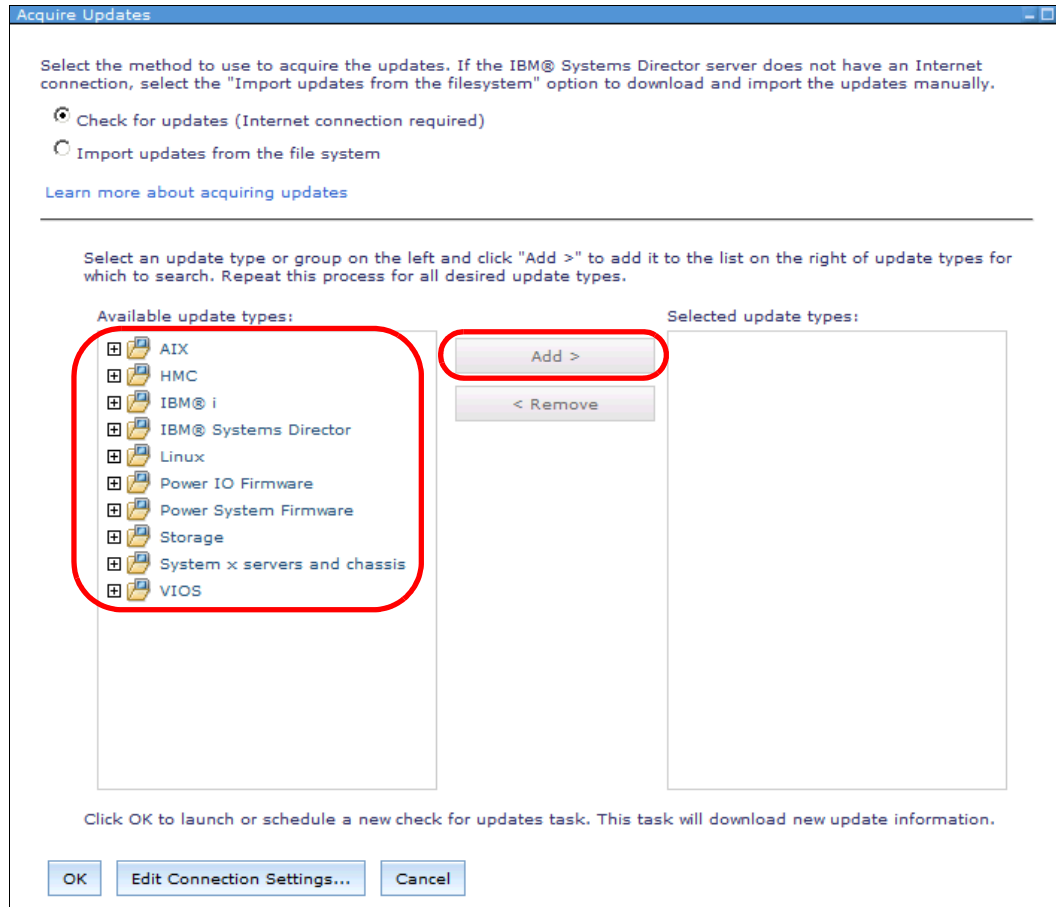


Figure 2-49 Select the updates for checking

5. After you select the updates that you want, click **OK**.
6. A scheduler window opens. Download the updates one time or define a recurring schedule (for example, once a week). We suggest that you perform the updates on a recurring schedule. The best time to update is off-hours so that this download traffic does not affect your daily business.

2.5.5 Update Manager with no Internet connection

If your Systems Director server does not connect to the Internet, you can use the Update Manager to import update packages. Download these update packages in advance from the IBM Fix Central website or another source for IBM updates.

IBM Fix Central is at this link:

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

You can obtain single updates (latest updates) or you can also use the UXSPI packages for your system. UXSPI packages contains updates for your system that are tested and work together. The types of updates include updates for UEFI, IMM, drivers, or firmware.

UXSPI packages are easier to download. You do not need to locate a download for each update package for each component in your system separately.

Follow these steps to apply the updates that you previously downloaded to Update Manager:

1. On the Update Manager startup page, select **Acquire updates** as shown in Figure 2-50.

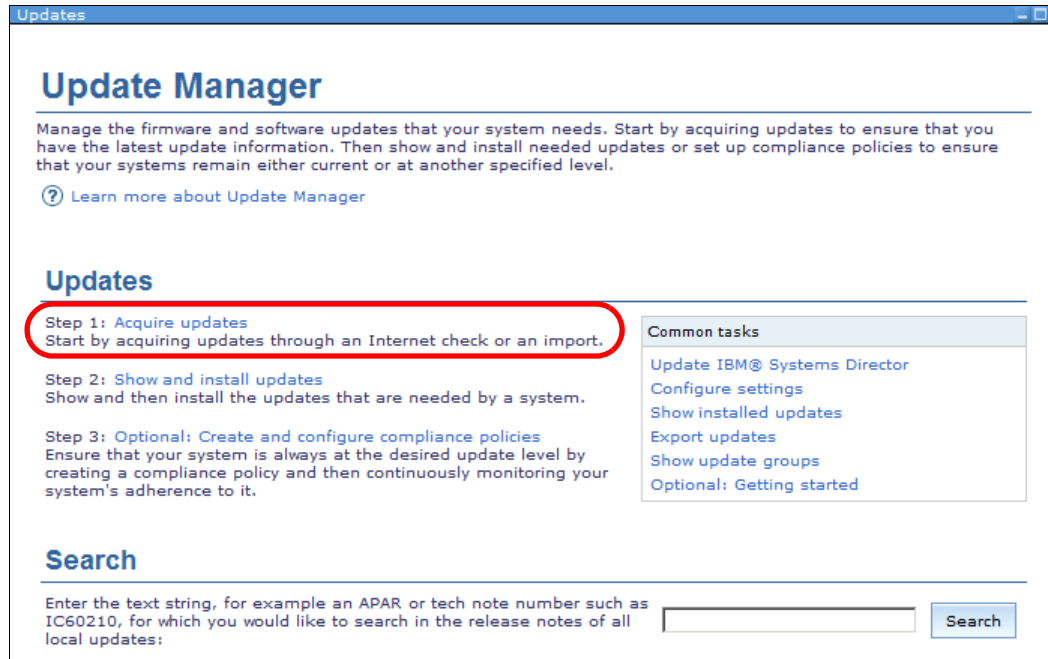


Figure 2-50 Acquire updates

2. Click **Import updates from the file system** as shown in Figure 2-51.

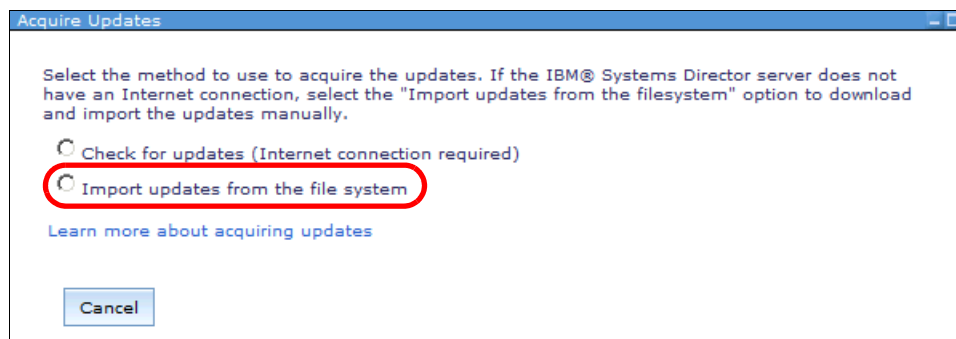


Figure 2-51 Acquire Updates selection window

3. When you select to import the updates, the window expands (Figure 2-52). Select the directory where you downloaded the updates previously. This directory must be on or accessible from the management server.

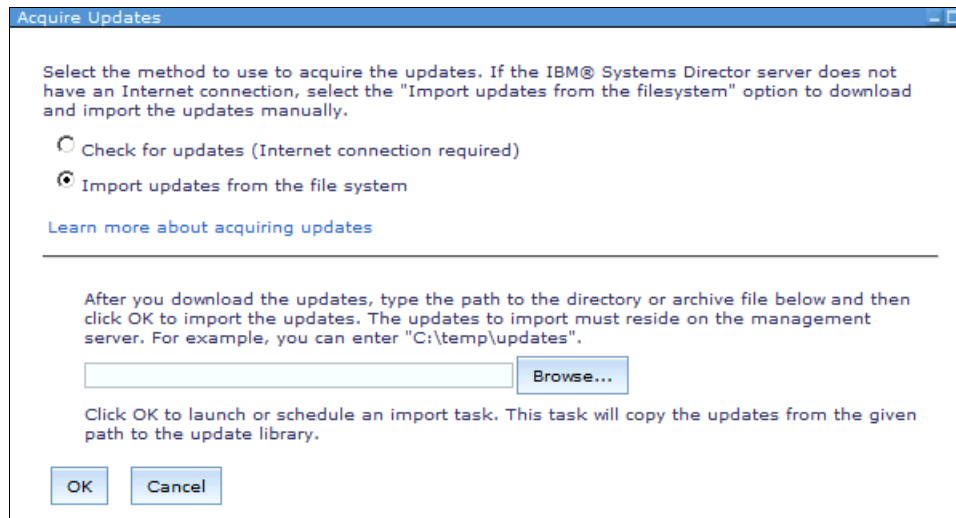


Figure 2-52 Import updates from the file system

4. After you select the directory, click **OK**. The updates are imported into the Systems Director server.

2.5.6 Compliance check

A *compliance check* compares information in the local repository of Systems Director with the inventory information that Systems Director collected from the managed systems. The compliance check process is a background process. After you define it, it runs automatically for each new update or for each new collection of system inventory information.

If the compliance check identifies new updates for a system, the system is marked as noncompliant with either an information, warning, or critical status. This status depends on the level of the system and the level of the available updates. This status can change if newer updates appear.

For the best results, schedule a regular download or import of the newest available updates and perform regular inventories for the available systems. You can automate this inventory collection for your systems as described in 2.4, “Inventory” on page 64.

You can set up a compliance check against a single system or a group of systems. If you use groups, define groups that contain systems of the same type or that share properties.

Follow these steps to set up the compliance check:

1. From the Update Manager main page, click **Optional: Create and configure compliance policies** as shown in Figure 2-53.

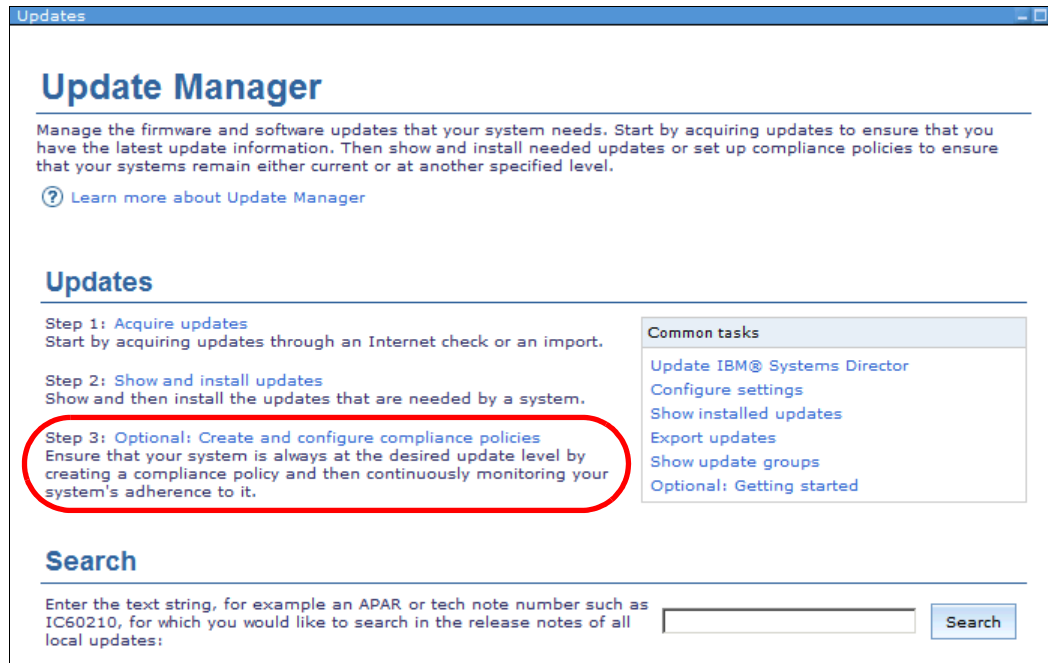


Figure 2-53 Select create and configure compliance policies

2. In Figure 2-54, select systems or a group for which you want to create the compliance check. After you select these systems or a group, click **OK**.

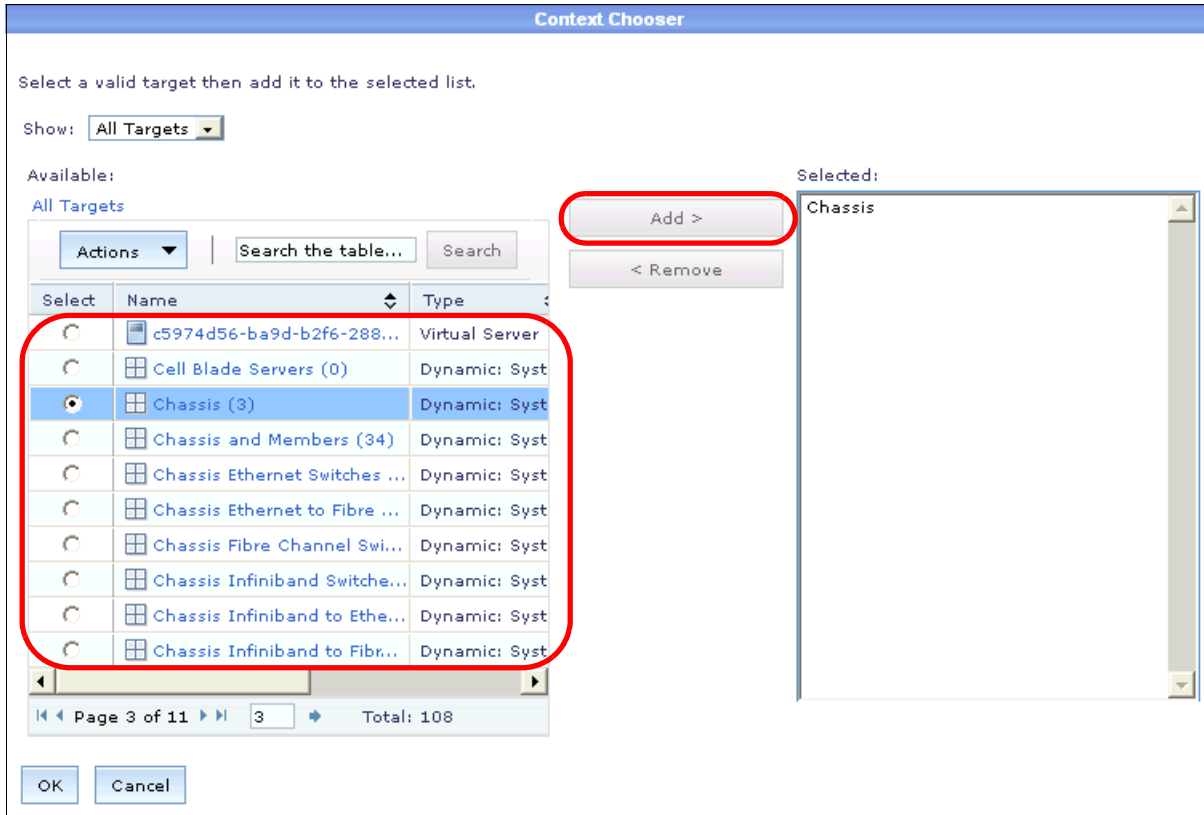


Figure 2-54 Select systems or a group for compliance check

If the group or systems that you select have no available inventory information, you see a message (Figure 2-55). The message states that no inventory is available and you need to perform an inventory collection by clicking **Collect Inventory**. After the inventory starts, click **Close Message**.

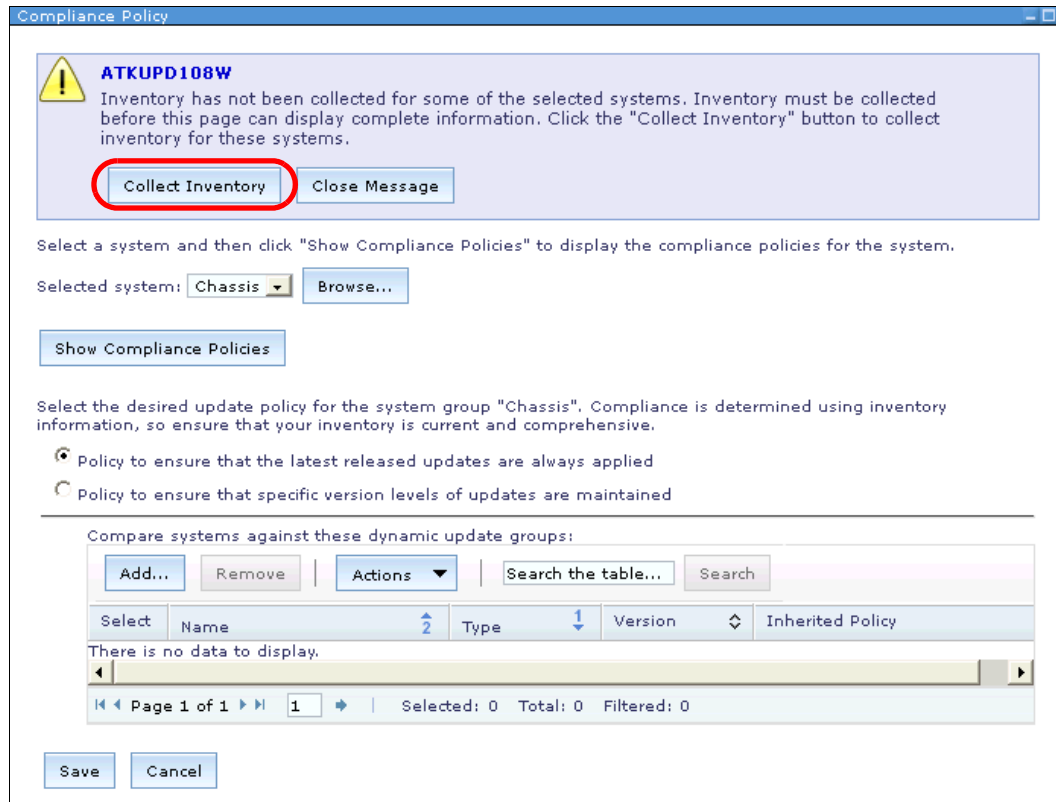


Figure 2-55 Warning message that no inventory is available

3. After the inventory run completes, a message appears and you can add a compliance policy for the systems or group that you selected before. Click **Add** (Figure 2-56).

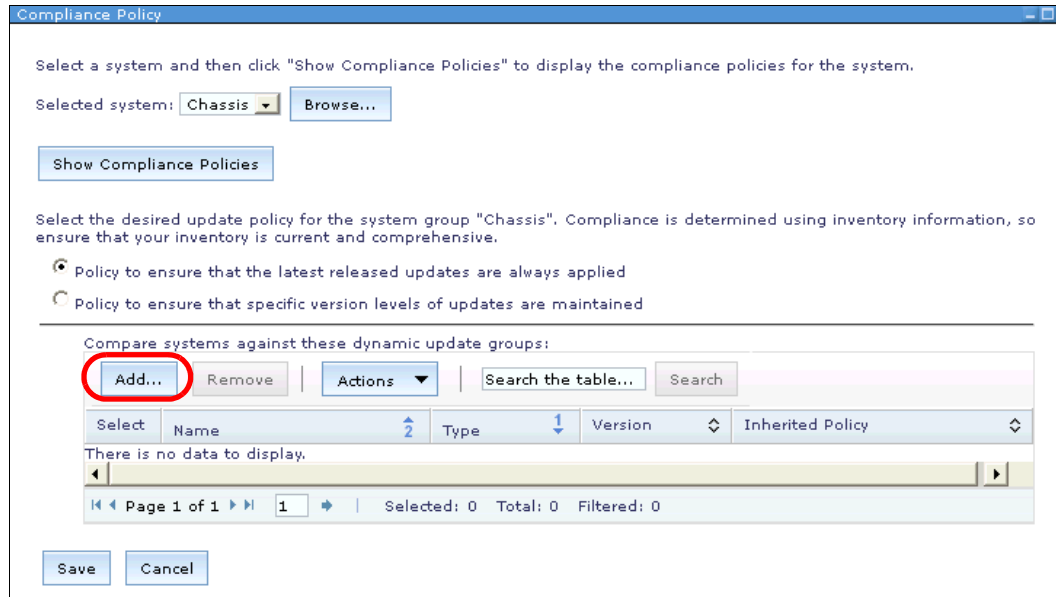


Figure 2-56 After you collect the inventory, select Add

4. In Figure 2-57, select the update group and click **Add**. This group defines the type of updates for which your system runs the compliance check. In our example, we selected All Critical IBM System x and BladeCenter updates and All IBM Systems Director 6.3 Updates. After you finish your selections, click **OK**.

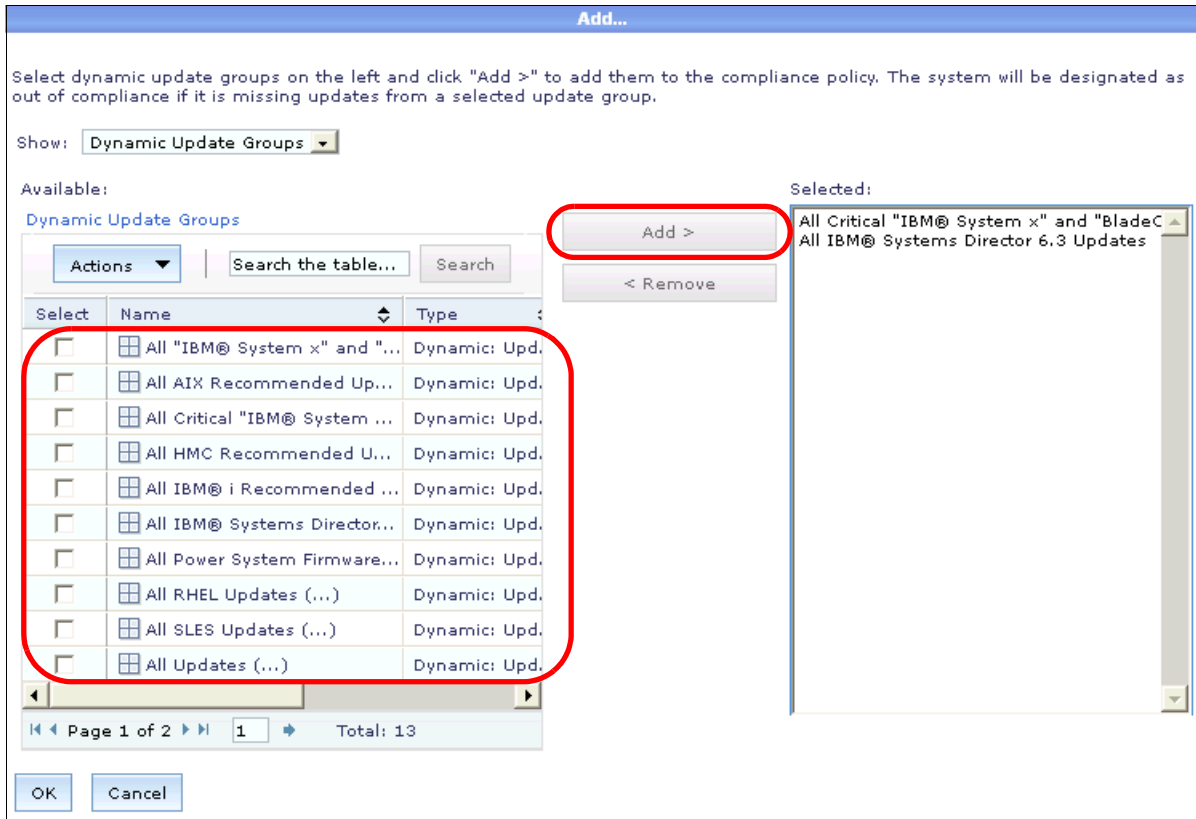


Figure 2-57 Select the update groups for the compliance check

5. You return to the previous window. The compliance policies that are defined for your systems are shown as seen in Figure 2-58. To finish the definition of the compliance policies, click **Save**.

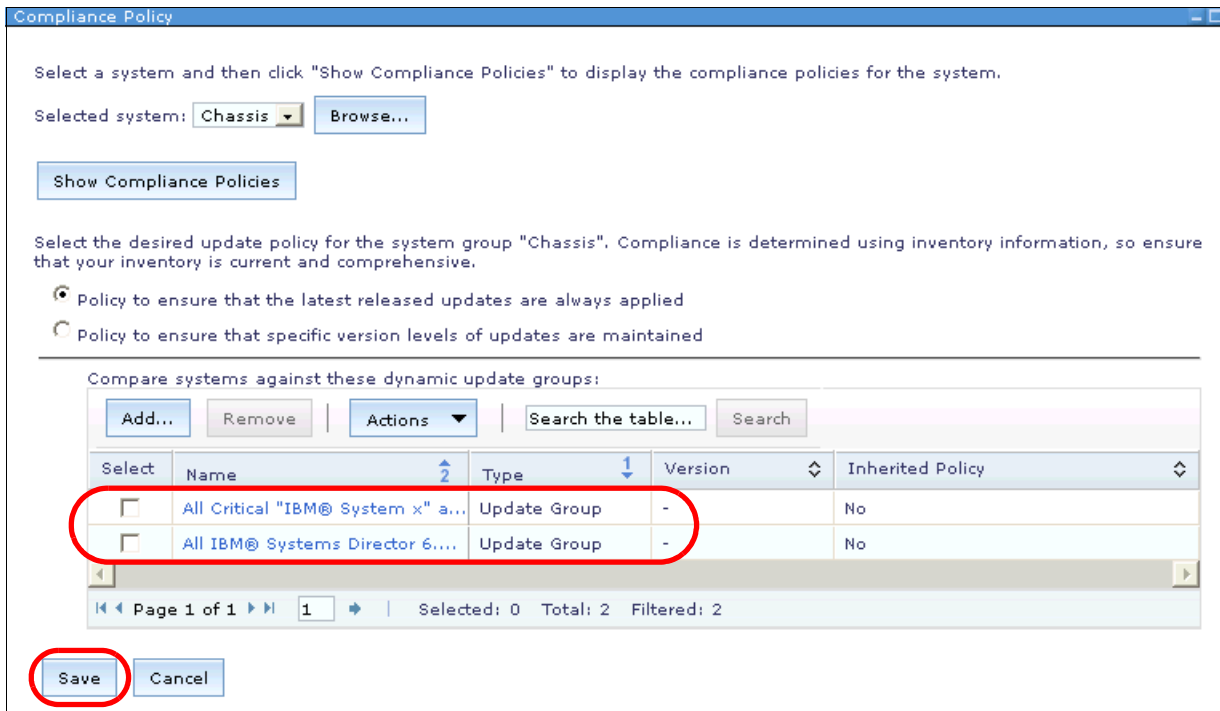


Figure 2-58 Selected update groups for the systems

- You return to the Update Manager home page where you see the Update Compliance section (Figure 2-59). You can see the compliance status of the systems that you specified.

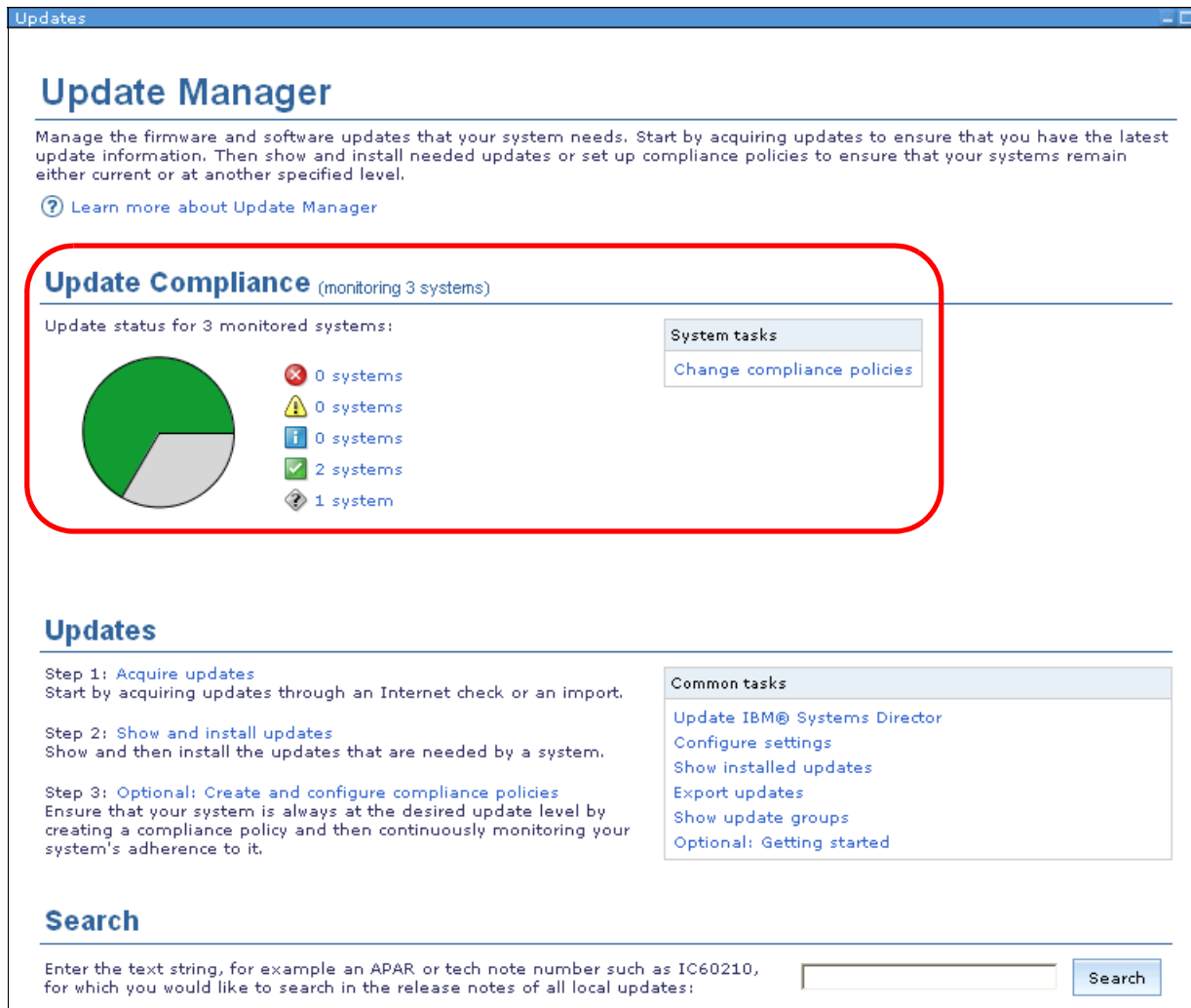


Figure 2-59 Update Manager with defined compliance check

2.5.7 Update process

The Update Manager is configured and you have the required updates (either from the Internet or imported from a local directory to the Systems Director repository). Start the update process.

We describe two methods:

- ▶ “Using Update Manager: Show and install updates” on page 101
- ▶ “Using the compliance check to update” on page 108

Using Update Manager: Show and install updates

You can check whether updates are available to install for systems or a group of systems:

1. From Update Manager, click **Show and install updates** as shown in Figure 2-60.

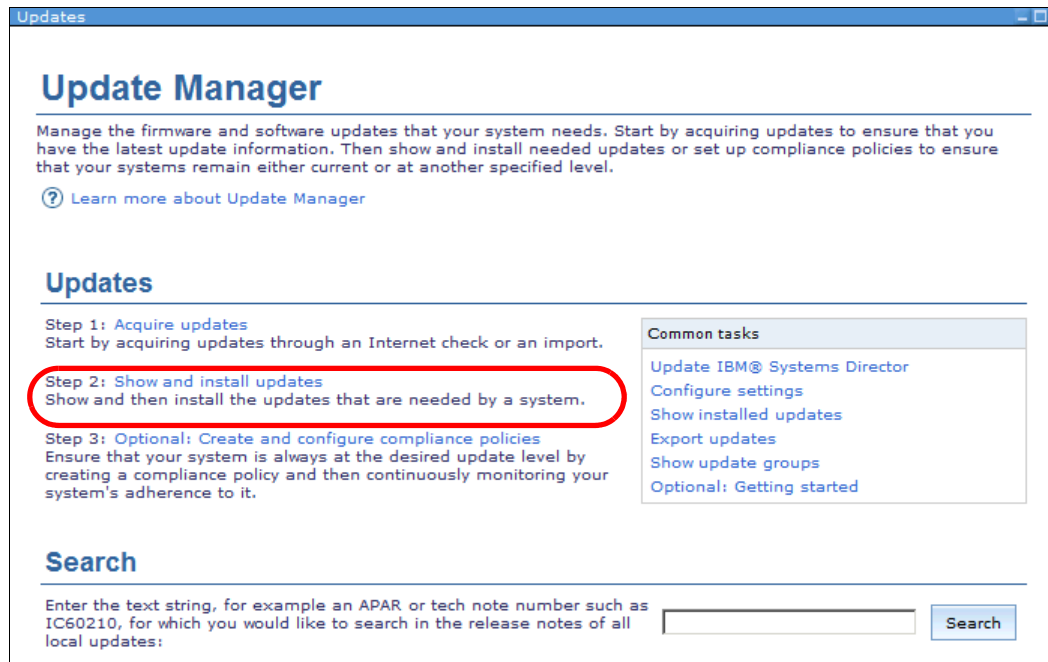


Figure 2-60 Update Manager: Show and install updates

2. Select the system or the group of systems for which you want to update. In our example, we select the Chassis group as shown in Figure 2-61. Click **Show and Install Updates**.

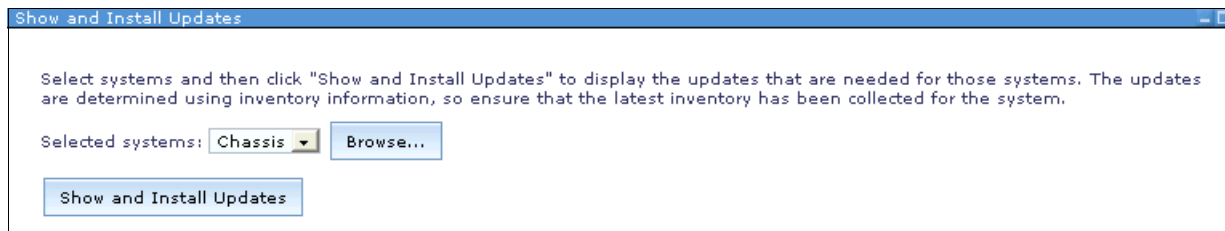


Figure 2-61 Show and Install Updates: System selection

3. The window expands to show the available updates for the systems that you selected. A message appears if no inventory is available for these systems. You can select to start the inventory collection.

In our example, the inventory was run before and one update is available for the group Chassis, which affects two systems (Figure 2-62).

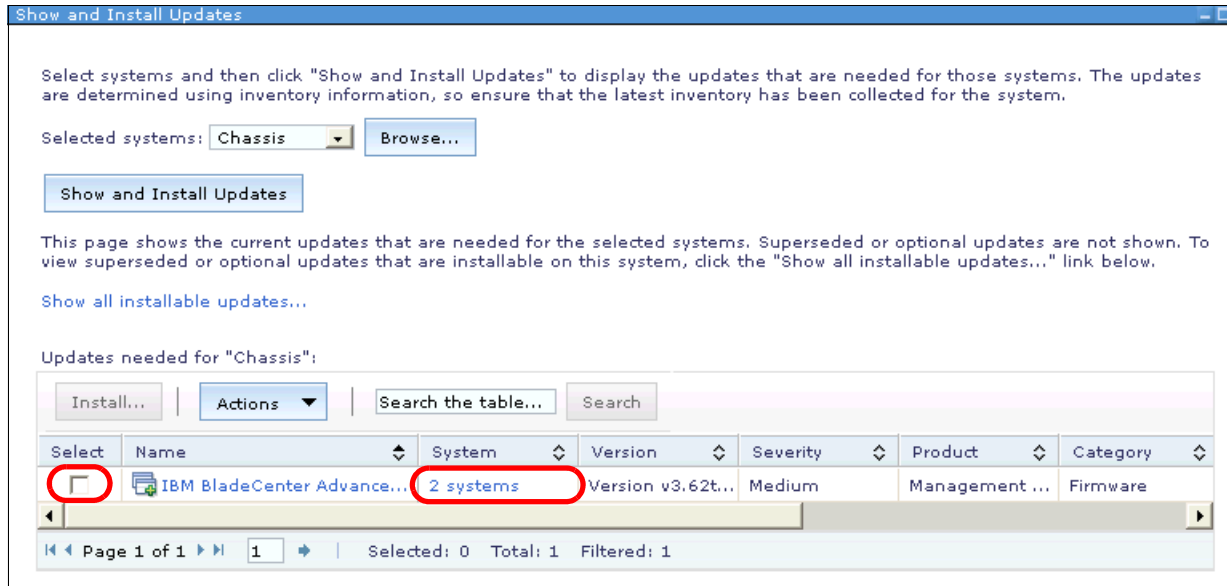


Figure 2-62 Show and Install Updates: Available update for selected systems

4. Multiple methods are available to install this update:
 - Click the check box next to the update package and click **Install**. This method is easiest and, in our example, updates two chassis.
 - But, because the update is available for two systems, you might want to know which system you are updating. Perhaps, you cannot update all systems at the same time for business reasons. You can click **2 systems** in the System column in Figure 2-62.

A new window opens where the two systems are listed as shown in Figure 2-63.

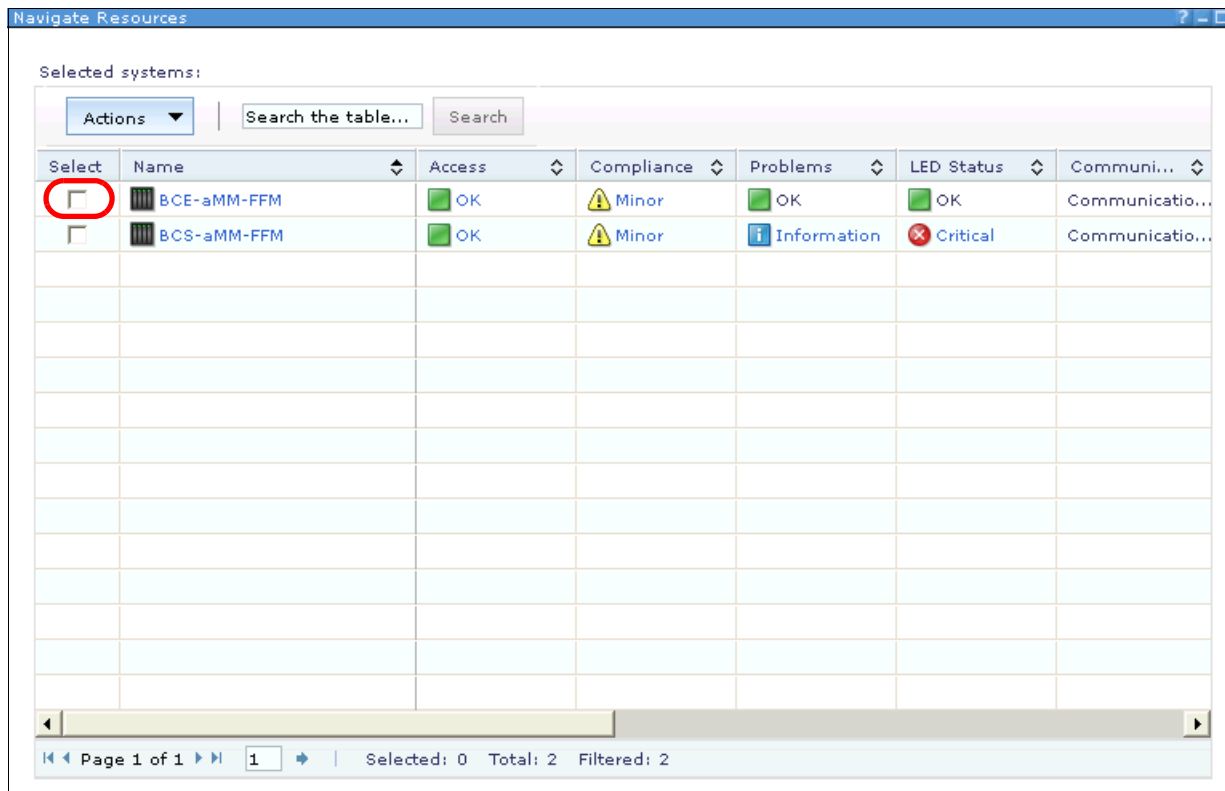


Figure 2-63 Updates for systems

Check the individual system or systems that you want to update and click **Actions** → **Release Management** → **Show and install updates**. This action returns you to the window that is shown in Figure 2-64. Click the check box next to the update and then click **Install** to start the upgrade installation process.

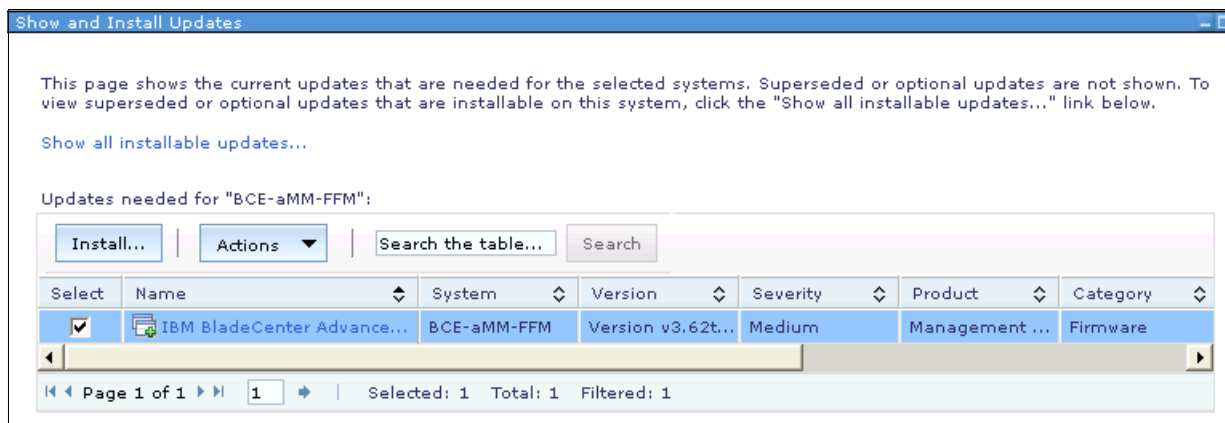


Figure 2-64 Select Install to start the installation process

5. For either method, the Install wizard opens (Figure 2-65). On the Welcome panel, click **Next** to proceed with the installation process.

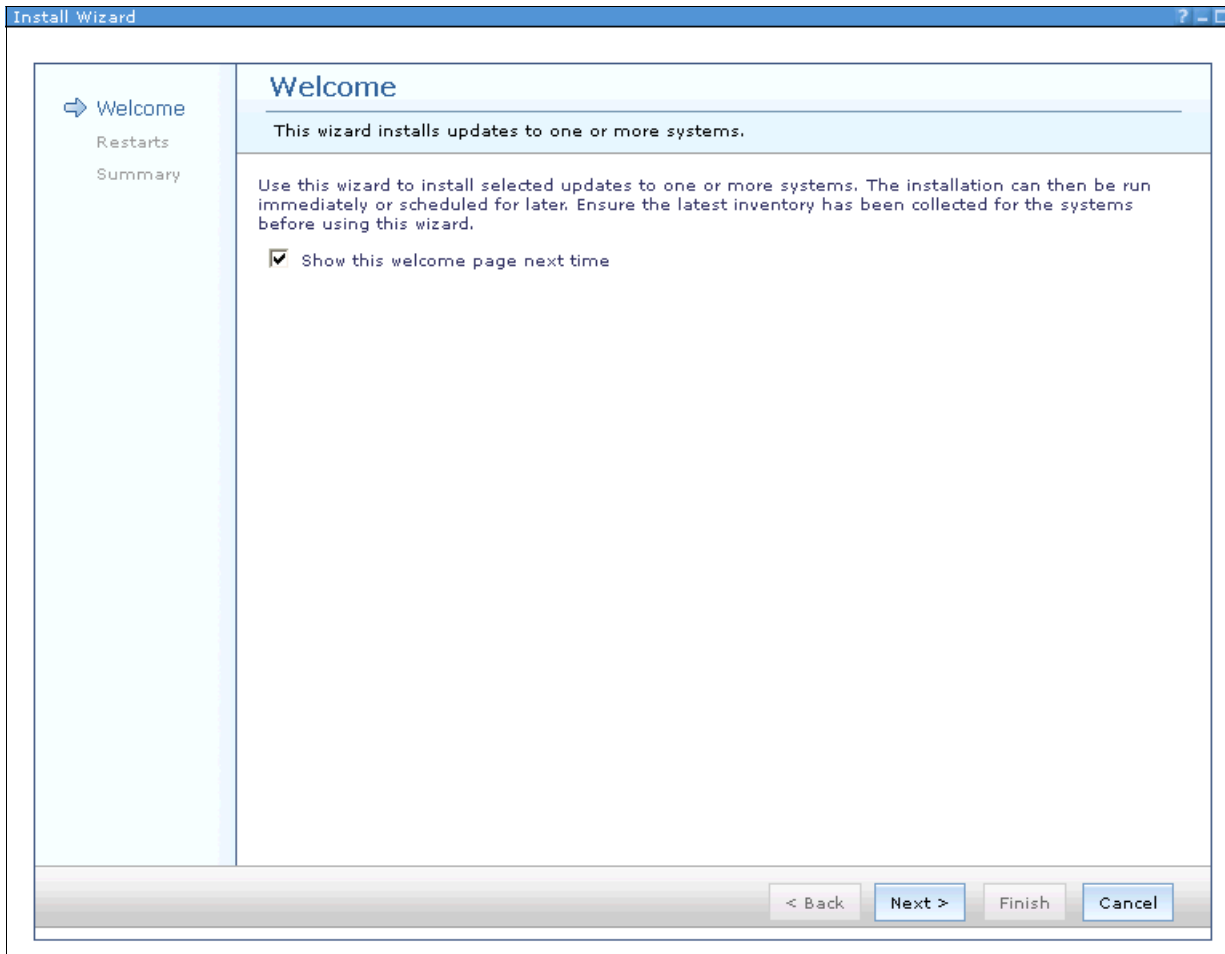


Figure 2-65 Install wizard Welcome panel

- On Figure 2-66, you see the selected system. By default, the update process automatically restarts the systems, if needed. The specific systems to update are listed and whether a restart is required is listed. If you clear the check box, the update is installed. However, you get an error message that the system is not restarted if a restart is required by the update process. You need to restart the system manually before the update takes effect. Click **Next** to continue.

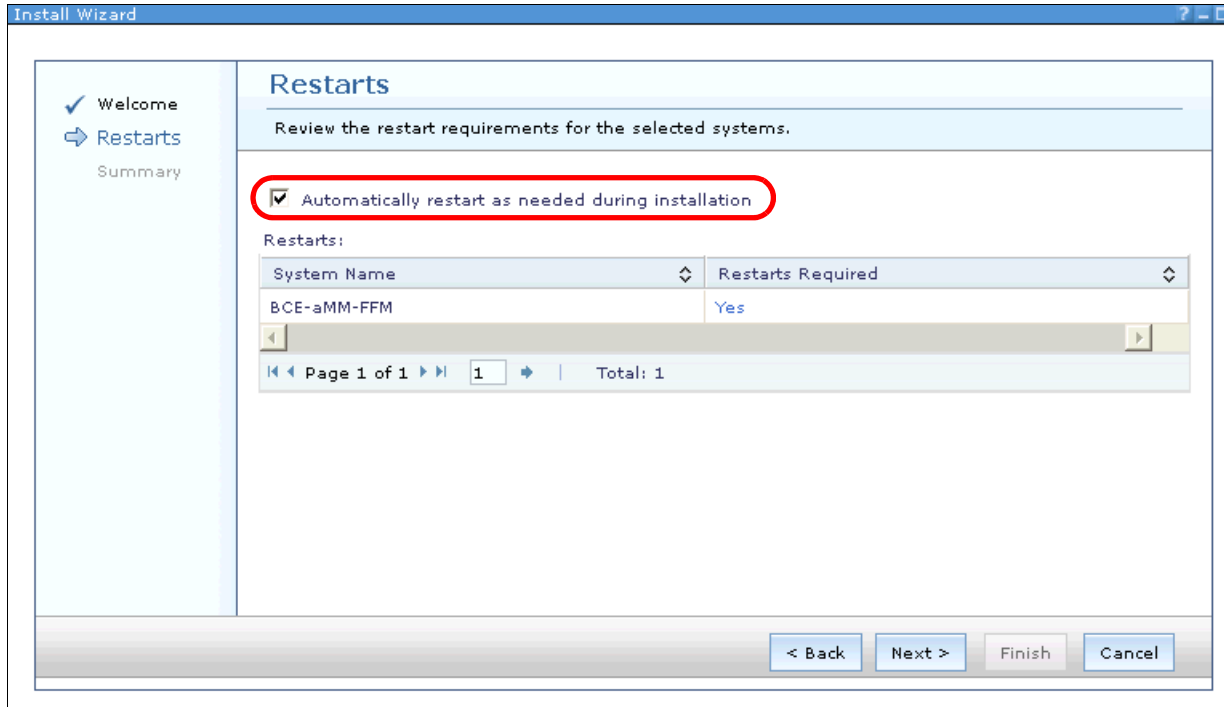


Figure 2-66 Install wizard: Restarts

7. A Summary window opens. Check the settings and the information of the update package. Click **Finish** to start the installation upgrade (Figure 2-67).

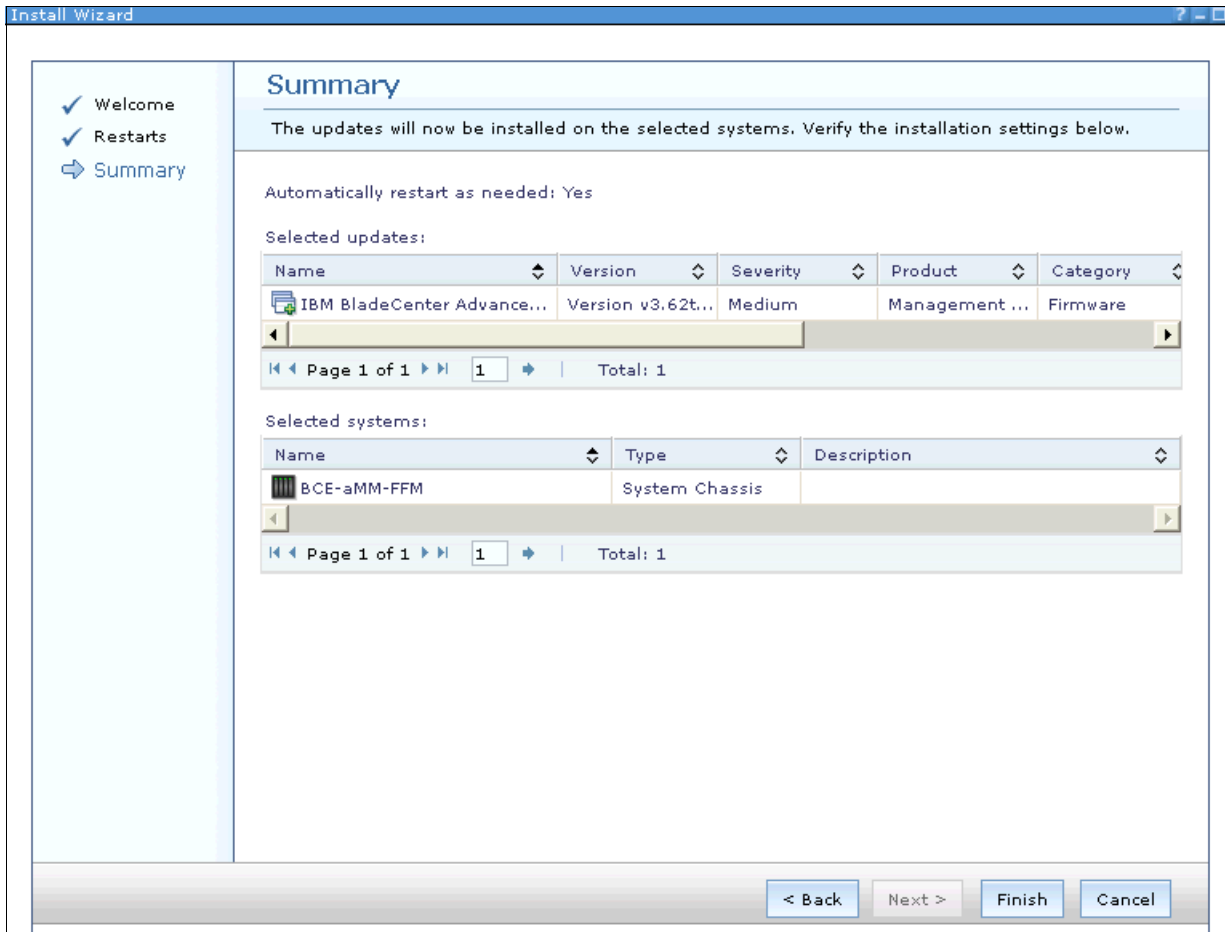


Figure 2-67 Install wizard: Summary

8. The Schedule tab opens. Select whether to run the update now or at a defined time (Figure 2-68).

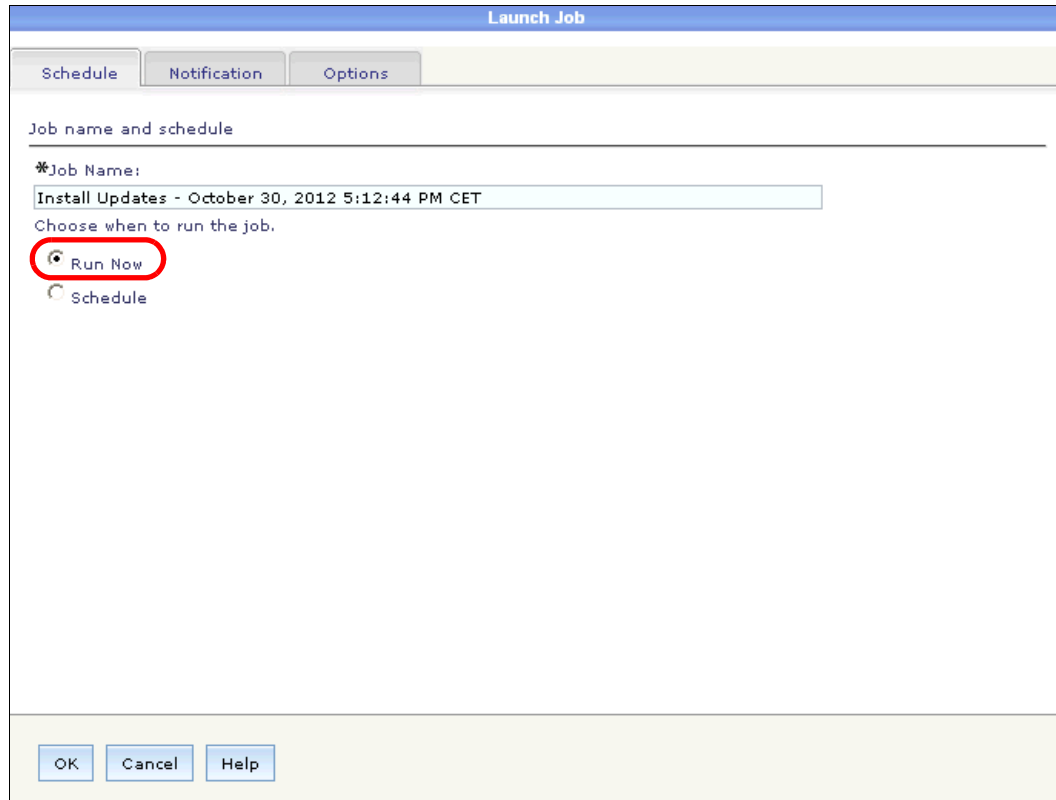


Figure 2-68 Schedule tab

9. If you select Run Now, a window opens where you can see that the job is created and started as shown in Figure 2-69.

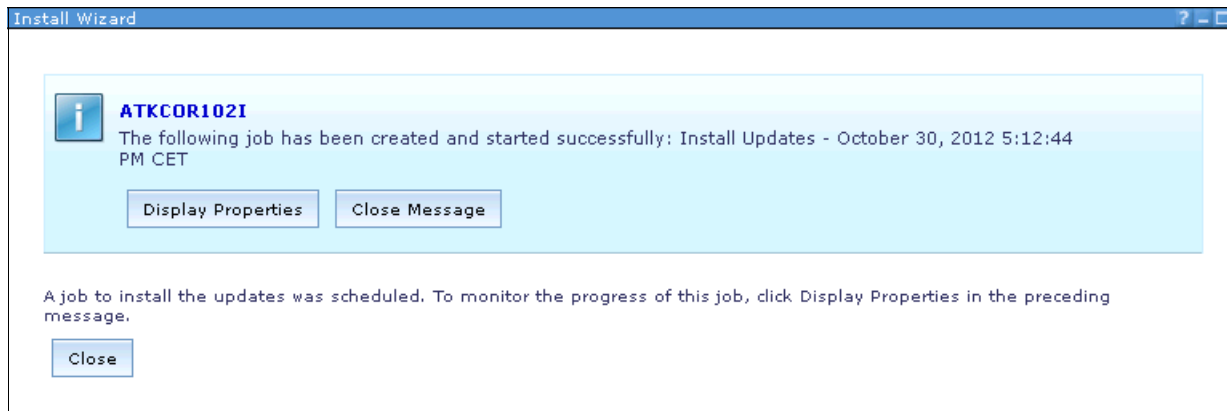


Figure 2-69 Job created and started

10. Click **Display Properties** to display the job properties where you can check the status and the log for the job (Figure 2-70). You can see that if the update was not downloaded before or imported, a download for the update package is started.

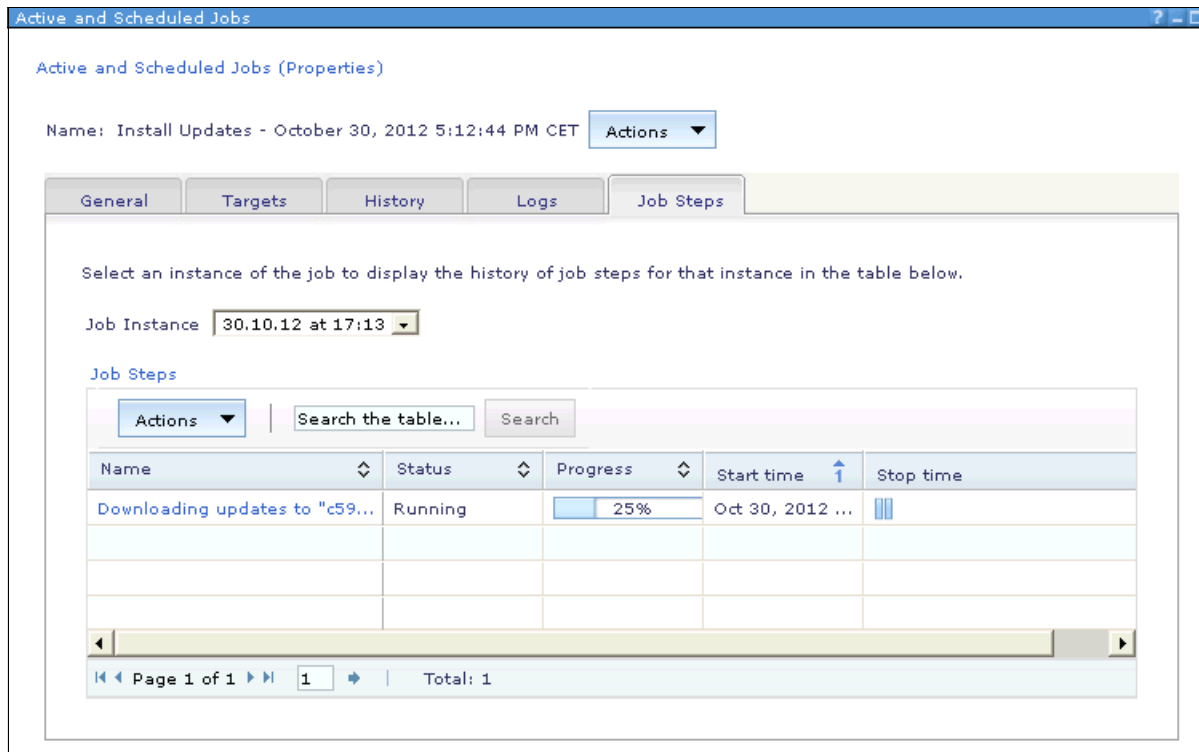


Figure 2-70 Active and Scheduled jobs (Properties): Job Steps tab to download updates

Using the compliance check to update

Compliance checks are described in 2.5.6, “Compliance check” on page 93). If you set up a compliance check and a system is noncompliant, start here to update your system.

Follow these steps to update systems from the compliance check:

1. Click the link beside the red, yellow (in our example), or blue icon from the compliance check that is shown in Figure 2-71.

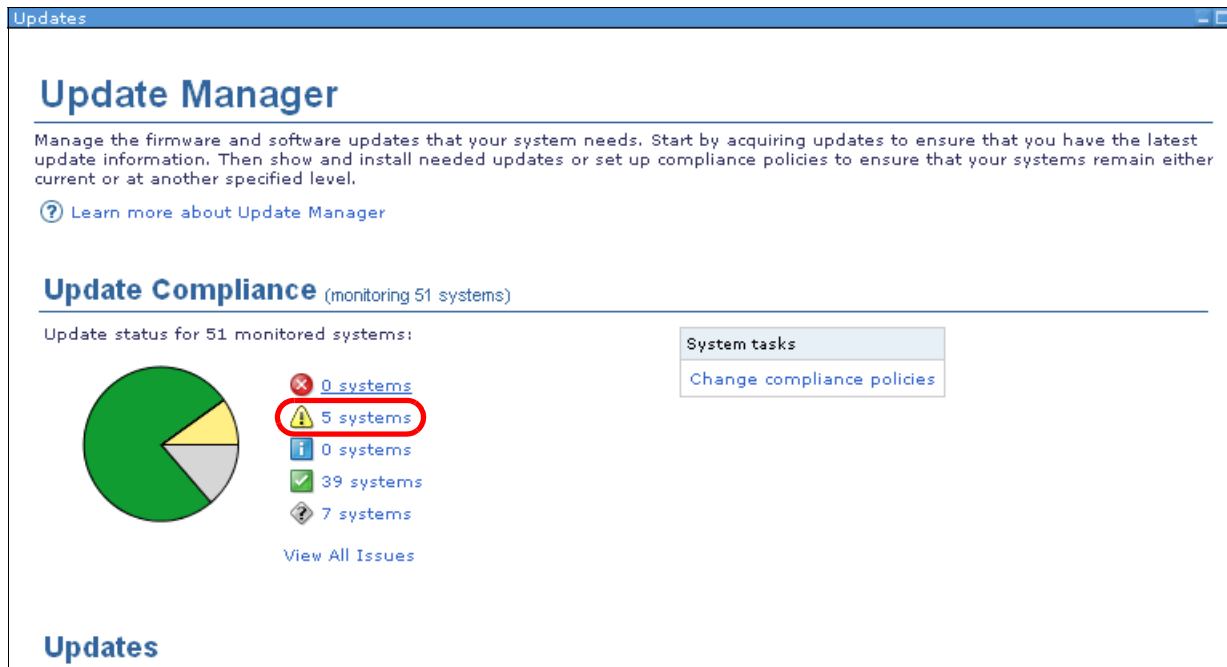


Figure 2-71 Compliance check: Select a system with a problem

- In the Navigate Resources window, you can see all the updates for the selected severity. Our example shows five systems with minor severity compliance issues (Figure 2-72). Click the check box next to the systems that you want to update. Then, click **Actions** → **Release Management** → **Show and Install updates**.

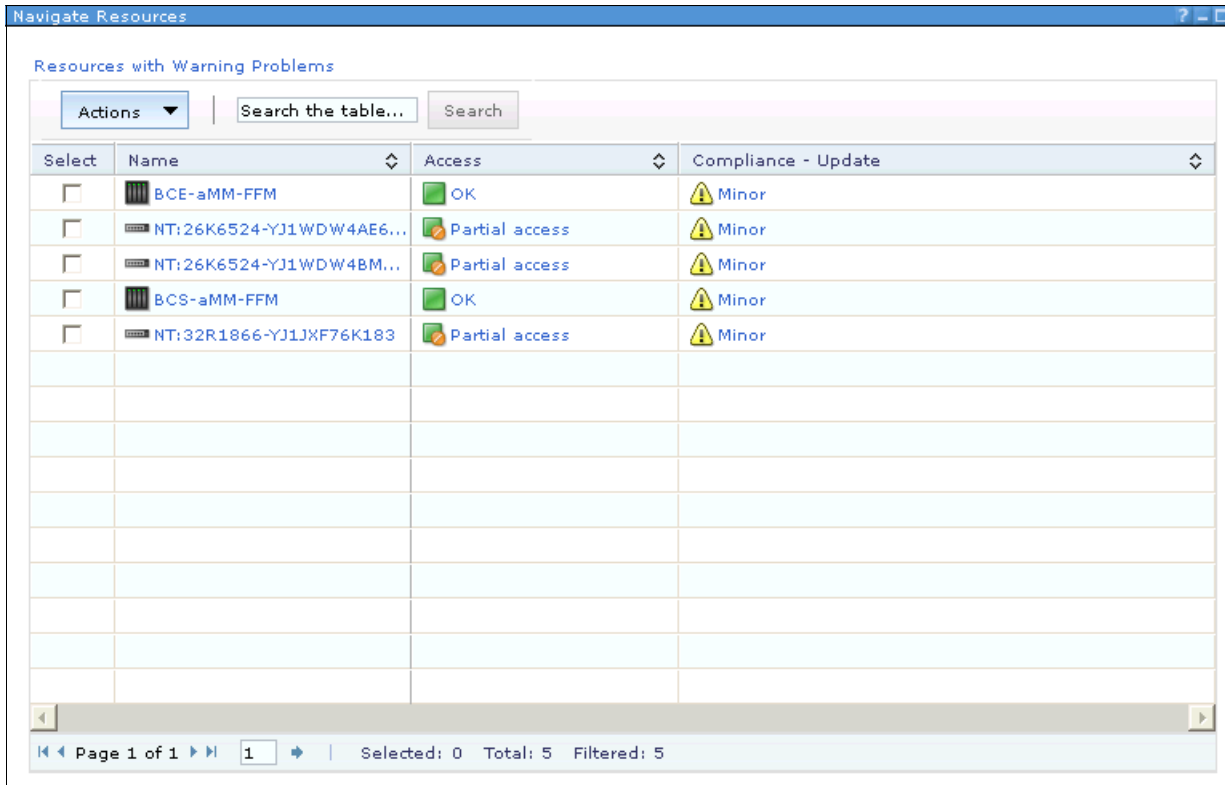


Figure 2-72 Compliance check: Systems with minor severity updates

- The Install wizard opens. The remaining steps are the same as described in “Using Update Manager: Show and install updates” on page 101, starting with step 5 on page 104.

Another way to update systems with compliance issues is to select the number beside the icon in the status bar on top of the Systems Director home page as shown in Figure 2-73.



Figure 2-73 Status bar: Compliance status

In step 3, select the Red Hat and SUSE/Novell Linux updates in Update Manager that you need for your systems as shown in Figure 2-75.

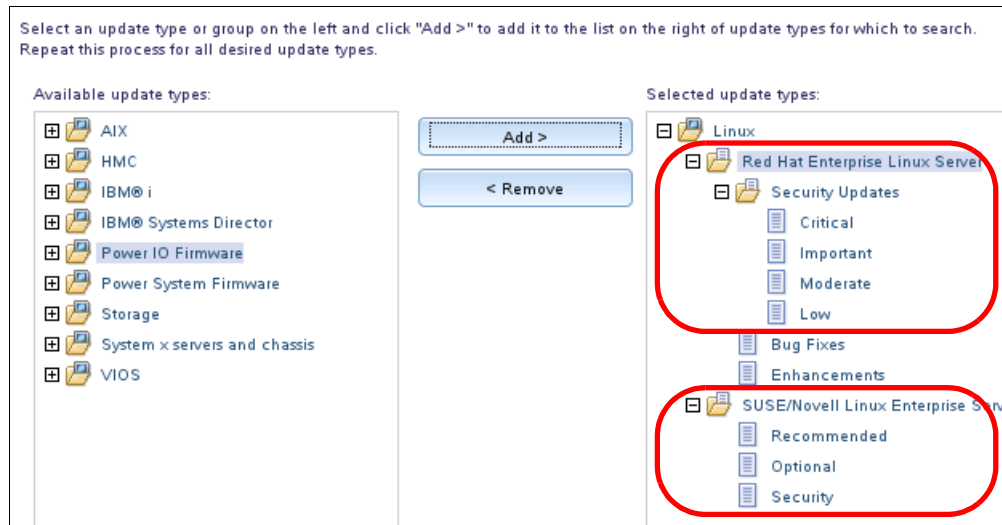


Figure 2-75 Select updates for Linux OS

You can also set a compliance check for your system for Linux updates. If the system discovers new Linux updates, use the same process for all other updates as described in 2.5.7, “Update process” on page 100.

Updating a system that runs AIX

The following page in the information center explains the requirements for updating AIX Systems:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.updates.helps.doc%2Ffqm0_c_um_considerations_for Updating_aix_systems.html

AIX updates can be downloaded automatically from within Systems Director or manually from Fix Central:

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

When you download AIX fixes, ensure that you review your download options. This step is critical to ensure that you select **Include informational files, and files required by Systems Director for installation**. These files are needed to manually import AIX updates to Systems Director from the command line.

The syntax for importing AIX updates is shown in Figure 2-76.

```
#smcli importupd -vr /tmp/updates/aix/7100-01-06-1241
```

Figure 2-76 Importing AIX updates

For updates for AIX, Update Manager is the focal point for centralized management and updates are performed by using NIM. Standard NIM troubleshooting procedures can be used, as needed.

Tip: If you import updates from a Network File System (NFS) mount, be careful with Secure Hash Algorithm (SHA). If the NFS mount is restricted, copy it locally to a temporary position on the Systems Director server and import to eliminate SHA warnings.

2.5.9 Updating the Systems Director server

If you want to update the Systems Director server, use the “Update IBM Systems Director” task. This task lets Update Manager use the defaults and run the update tasks for you automatically.

This task is accessible from the Systems Director home page (Figure 2-77) and also from the Update Manager page (Figure 2-78 on page 114).

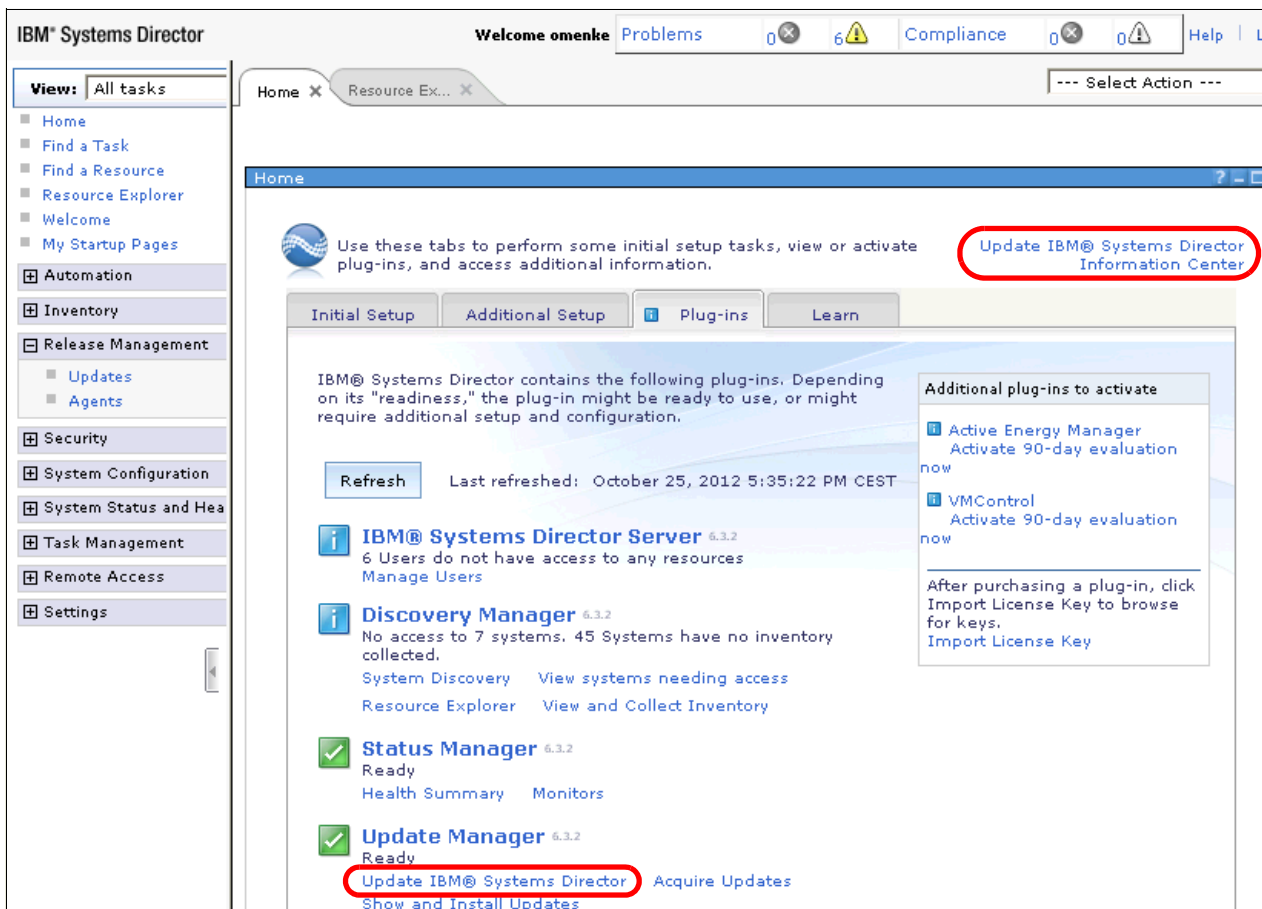


Figure 2-77 Launching Update Systems Director from the home page

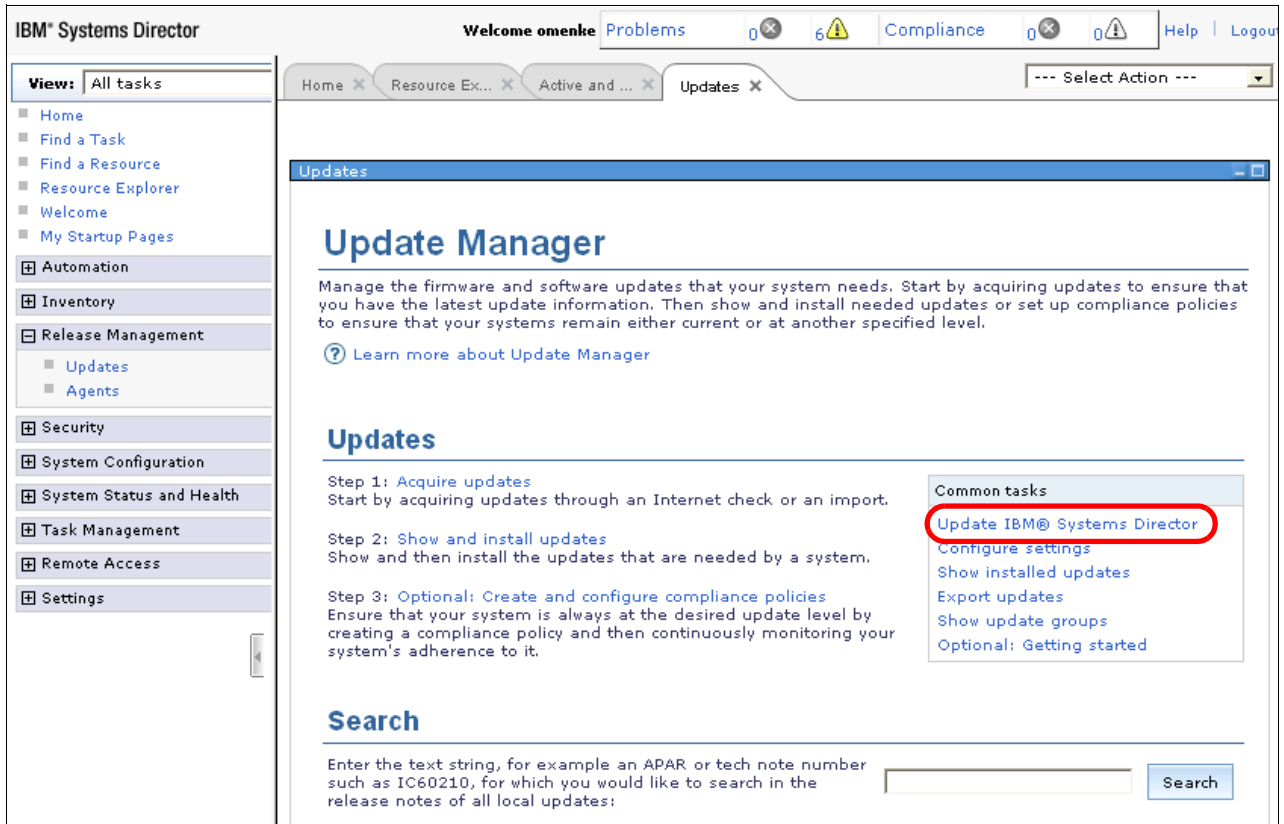


Figure 2-78 Launching Update Systems Director from the Update Manager page

When you launch the update task, the system checks for available updates as shown in Figure 2-79.



Figure 2-79 Update status for Systems Director update

If no new updates are available, you see a message that is similar to Figure 2-80.

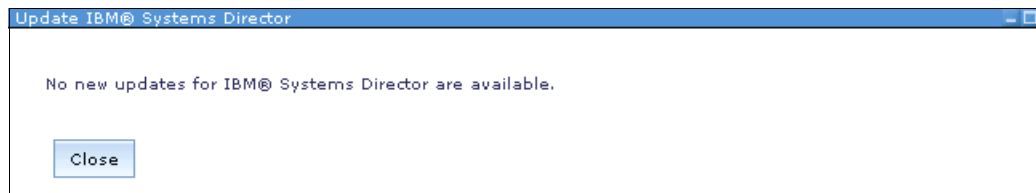


Figure 2-80 No updates are available

If new updates are available for your Systems Director server, you see a window similar to Figure 2-81.

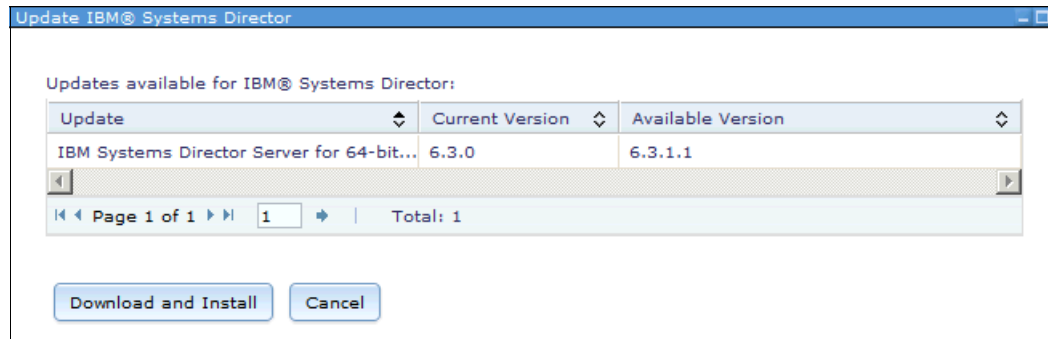


Figure 2-81 Update Systems Director

Follow these steps to install the updates:

1. Click **Download and Install** in Figure 2-81. You are reminded to back up your server (Figure 2-82). We explain how to perform a backup in Chapter 4, “Backup” on page 219.

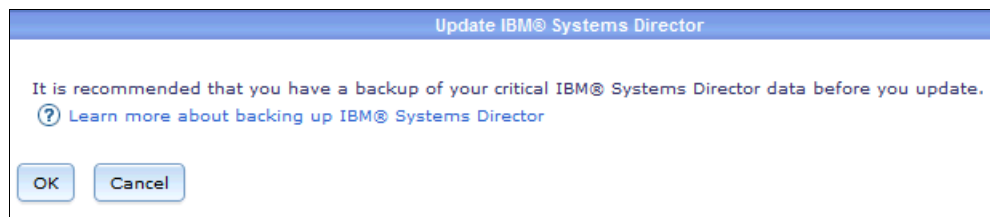


Figure 2-82 Information window about backup

2. Click **OK** to proceed to the Schedule window. Select **Run Now** and the updates are downloaded and installed. Or, you can schedule the update to be performed in off-hours. The status of the task is under **Task Management** → **Active and Scheduled Jobs**.
3. After the upgrade completes, the Systems Director server must be restarted. The best method is to use one of the following command-line commands:
 - Windows:


```
net stop dirserver
```

 Stop the Systems Director server.

```
net start dirserver
```

 Start the Systems Director server.
 - Linux and AIX:


```
smstop
```

 Stop the Systems Director server.

```
smstart
```

 Start the Systems Director server.
4. To check the status of the Systems Director, use the following command:
 - Windows:

The status icon is on the Windows panel. Use the `smstatus.bat (-r)` command to see the status and the update of the status.
 - Linux and AIX:

Use the `smstatus (-r)` command to see the status.

After the Systems Director server restarts, check whether the new version is installed and running. Check the version beside each manager on the home page. Or, check the `version.srv` file in the directory where the Systems Director server is installed.

2.5.10 Command-line tools

Command-line tools are available for Update Manager as listed in Table 2-19.

Table 2-19 Command-line tools for Update Manager

Command	Description
checkupd	Check changed and superseding updates.
cleanup	Clean (that is, delete) update files and information in the local update library.
importupd	Import updates into the update library on the management server. This command is used if no internet access is available.
installneeded	Update the Systems Director server and agents or to install other types of updates.
installupd	Install one or more updates to one or more systems.
lsupd	List the available updates and their attributes.
lsver	List the current version and, if you updated the product, the previous version of Systems Director that is installed on the system.
uninstallupd	Use to uninstall (roll back) an update on a specific system if the update package supports the rollback.

For detailed information about all the **smcli** command-line commands that are used for the Update Manager and their options, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_update_cmds.html

Certain functions are only available by using the command line. One example is cleaning or deleting the local update library. Use this function if multiple downloaded updates are not used or if you are running out of storage. After you clean the library, run a check for updates to fill the library with new update information. *The information from the library is used for the compliance check.*

In Example 2-1, we clean up the library and then we start a check for new updates from the command line. You can also run the check for new updates in the browser interface as described in 2.5.4, “Update Manager with Internet connection” on page 89.

In our example, we first list the updates that are downloaded to the local update library with the **smcli lsupd** command. For brevity in our example, some output lines are not displayed (200 packages are available).

Example 2-1 *smcli lsupd*

```
PS C:\Windows\system32> smcli lsupd
SysDir6_3_1_Platform_Agent_Windows
SysDir6_3_1_Platform_Agent_xLinux
SysDir6_3_Platform_Agent_AIX
SysDir6_3_Platform_Agent_Windows
SysDir6_3_Platform_Agent_pLinux
SysDir6_3_Platform_Agent_xLinux
SysDir6_3_Platform_Agent_zLinux
agentmanager.feature_6.3.1
bnt_fw_bcsw_110gup-6.3.1.1_anyos_noarch
bnt_fw_bcsw_110gup-7.2.2.0_anyos_noarch
```

```
bnt_fw_bcsw_24-10g-6.9.1.0_anyos_noarch
bnt_fw_bcsw_24-10g-7.2.2.0_anyos_noarch
bnt_fw_torsw_g8264-6.8.4.0_anyos_noarch
bnt_fw_torsw_g8316-6.8.4.0_anyos_noarch
brcd_fw_6.3.1-dcb2_anyos_noarch
brcd_fw_bcsw_sansm-505a_anyos_noarch
cigesm-i6q412-tar.121-22.ea13
com.ibm.aem.common_4.4.1
com.ibm.aem.console_4.4.1
.....
```

Then, we clean up the library by using the `smcli cleanupd -am` command as listed in Example 2-2. This command needs time to delete all packages and remove the index file. After we run the cleaning of the local library (`smcli cleanupd -am`), we check with the `smcli lsupd` command whether update packages are still available. You can see in the example that after cleaning, no installation package is available.

You can clean up only one or some of the installation packages that are in the local library. Use `-w %packagename%` instead of the `-am` option.

Example 2-2 smcli cleanupd

```
PS C:\Windows\system32> smcli cleanupd -am
PS C:\Windows\system32> smcli lsupd

PS C:\Windows\system32>
```

We start to download new packages by using the `smcli checkupd -a` command, which checks the IBM repository for all updates. You can also use other options, such as the `-N groupname`, to check only for updates for a member of a defined group (Example 2-3).

Example 2-3 smcli checkupd

```
PS C:\Windows\system32> smcli checkupd -a
PS C:\Windows\system32>
```

The `-a` option needs a long time to finish. No output is listed during the download process if it is run on the command line. You can see that the command is finished only when a new command prompt is visible.

When the command is finished, check which updates are downloaded by running the `smcli lsupd` command (Example 2-4). You can see examples from the listing to show the different types of updates that are downloaded. In our example, over 500 update packages are available (for Linux, AIX, firmware, driver, Director, and VIOS).

Example 2-4 smcli lsupd with examples for different downloads

```
PS C:\Windows\system32> smcli lsupd
01AF743_100_100
01AF743_105_100
....
032512EE02F845008725779E00509382_AIX
032512EE02F845008725779E00509382_LNX
03F50ADC70A9CEA9872577B200727962_AIX
....
MH01084
MH01097
MH01101
MH01102
```

```
....
U823341
U824377
U824378
....
VIOS_2.2.1.3-FP25-SP01
VIOS_2.2.1.4-FP25-SP02
VIOS_2.2.2.1-FP26
....
agentmanager.feature_6.3.1
....
bnt_fw_bcsw_110gup-6.3.1.1_anyos_noarch
bnt_fw_bcsw_110gup-7.2.2.0_anyos_noarch
bnt_fw_bcsw_24-10g-6.9.1.0_anyos_noarch
.....
com.ibm.aem.common_4.4.1
com.ibm.aem.console_4.4.1
com.ibm.aem.discovery_4.4.1
....
com.ibm.director.storage.storagecontrol.member.AIX_4.2.2.build-00119
com.ibm.director.storage.storagecontrol.member.Linux_4.2.2.build-00095-20120516-iFix
....
cisco_fw_bcio_12.2.50se1_anyos_noarch
ibm_fw_amm_bpet62t_anyos_noarch
ibm_fw_bcio_N4K_4.1.2.E1.1i_anyos_noarch
ibm_utl_uxspi_9.21_rhel5_32-64
ibm_utl_uxspi_9.21_sles11_32-64
ibm_utl_uxspi_9.21_winsrvr_32-64
```



Advanced functions

Several of the more advanced features that IBM Systems Director offers are described. The following topics are covered:

- ▶ 3.1, “Hardware Management Console and AIX Launch-in-Context” on page 120
- ▶ 3.2, “Light path diagnostics” on page 134
- ▶ 3.3, “Hardware logs” on page 139
- ▶ 3.4, “Service and Support Manager” on page 143
- ▶ 3.5, “Event logs” on page 150
- ▶ 3.6, “Automation Manager” on page 160
- ▶ 3.7, “Security” on page 190

3.1 Hardware Management Console and AIX Launch-in-Context

Information about the discovery of a Hardware Management Console (HMC) and the HMC managed resources is described. The HMC Launch-in-Context (LiC) capability and extended tasks are shown.

The Systems Director server can be used for a wide range of tasks on systems that are under the control of a managed HMC:

- ▶ Creating virtual servers
- ▶ Editing virtual server resources
- ▶ Views
- ▶ Topology

Discovering an HMC by using the Systems Director server offers a *single-pane-of-glass* view to monitoring and supporting Power Systems hardware. Some dynamic LPAR (DLPAR) functions are embedded in the Systems Director UI and other functions can be initiated by using LiC.

Before you begin

Before the discovery of the HMC, carefully determine what level of access is passed to the Systems Director server. This determination relates to the tasks that are required to manage the HMC.

Use the following links to the information center to set up:

- ▶ Setting up user access:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.vim.helps.doc%2Feica7_t_setting_up_user_access_hmc.html

- ▶ Configuring the HMC:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.vim.helps.doc%2Feica7_t_configuring_hmc.html

- ▶ Managing systems that are controlled by HMC LiC:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.power.helps.doc%2Ffqm0_t_managing_hmc_ivm.html

- ▶ Preparing the HMC for discovery:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.install.helps.doc%2Ffqm0_t_preparing_hmc_for_discovery.html

Discovery

Discovery of the HMC is performed by way of the normal discovery process. Resources are discovered by either IP address or host name.

The following steps show the process:

1. From the UI on Systems Director, select **Inventory** → **System Discovery** (Figure 3-1).

Name	Discovered	Type	Access	Problems	Compliance
hmc-itso	New	Hardware Manag...	No access	OK	OK

Figure 3-1 Discovered appliances

2. Authenticate with the HMC by using a user ID as shown in Figure 3-2.

Specify the user ID and password to authenticate Systems Director to one or more target systems. Then click Request Access to grant all authorized

*User ID:

*Password:

Selected targets:

Name	Access	Trust State
hmc-itso	No access	<input type="checkbox"/> Not applicable

Page 1 of 1 | 1 | Total: 1

Figure 3-2 Request Access

3. If the HMC user access is set up correctly and the correct settings are enabled on the HMC Network settings, access displays OK.
4. To view the recently discovered HMC and associated Power Systems, use the Systems Director UI and click **Inventory** → **Views** → **Platform Manager and Members**.

Terminology: For a list of the terminology that is used in Systems Director for Power Systems users, see this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.power.helps.doc%2Ffqm0_c_power_new_terms.html

- The view is automatically populated with the resources that are visible to the user ID on the HMC (Figure 3-3).









Platform Managers and Members						
Platform Managers and Members (View Members)						
<input type="button" value="Actions"/> <input type="text" value="Search the table..."/> <input type="button" value="Search"/>						
Select	Name	Access	Problems	Compliance	IP Addresses	Type
<input type="checkbox"/>	 hmc-itso	 OK	 OK	 OK	9.5.167.165, 172.16...	Hardware Manage...
<input type="checkbox"/>	 itso-power	 OK	 OK	 OK		Server

Figure 3-3 Platform Managers and Members

- From the Systems Director UI, see an expanded view for Power Systems servers by clicking **Inventory** → **Views** → **Virtual Servers and Hosts**, as shown in Figure 3-4.










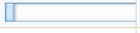




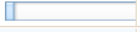









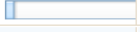
Virtual Servers and Hosts								
Virtual Servers and Hosts (View Members)								
<input type="button" value="Performance Summary"/> <input type="button" value="Actions"/> <input type="text" value="Search the table..."/> <input type="button" value="Search"/>								
Select	Name	State	Access	Problems	Compliance	OS Type an...	CPU Utilizat...	Processors
<input type="checkbox"/>	 itso-power	Started	 OK	 OK	 OK			
<input type="checkbox"/>	 itso-aix00	Started	 OK	 OK	 OK	AIX 6.1		
<input type="checkbox"/>	 itso-aix01	Started	 OK	 OK	 OK			
<input type="checkbox"/>	 itso-aix02	Started	 OK	 OK	 OK			
<input type="checkbox"/>	 itso-vio	Started	 OK	 OK	 OK			

Figure 3-4 Virtual Servers and Hosts

- Because the HMC is discovered, we get visibility to the HMC menu by Launch-in-Context as shown in Figure 3-5.

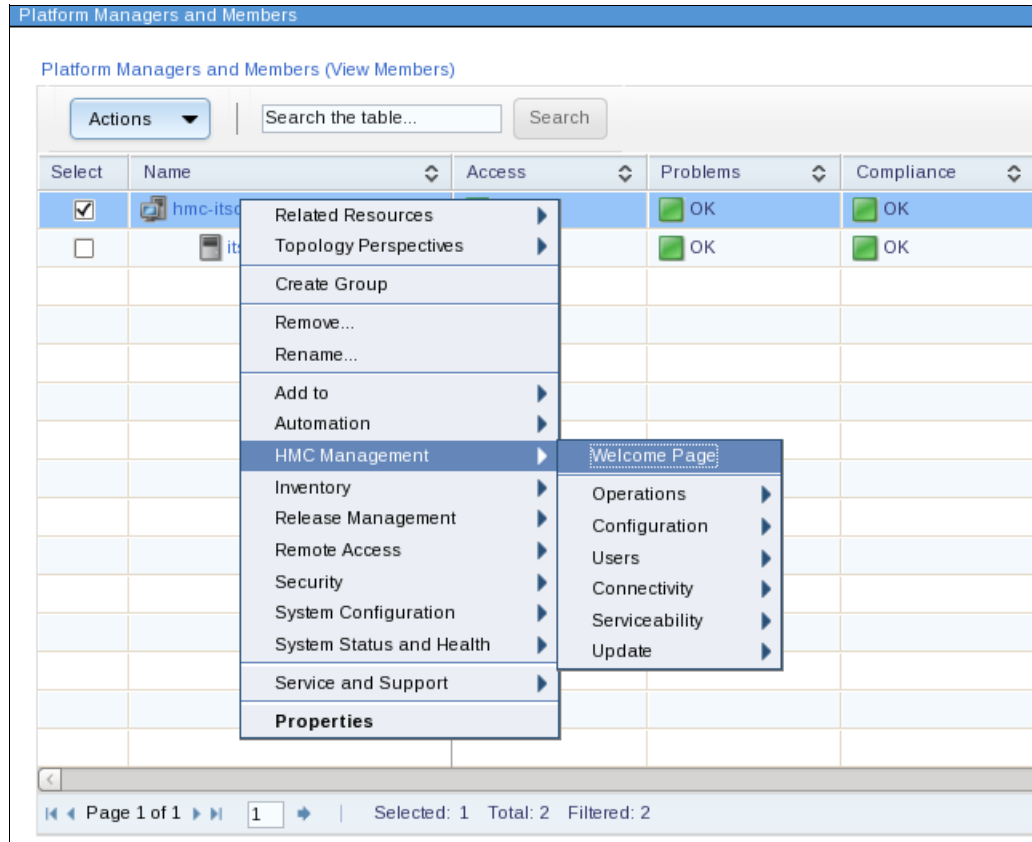


Figure 3-5 HMC menu

- If we select the Welcome Page from the HMC menu, it does not launch (Figure 3-6). We still do not have full authentication to use the HMC and need to configure single sign-on (SSO).

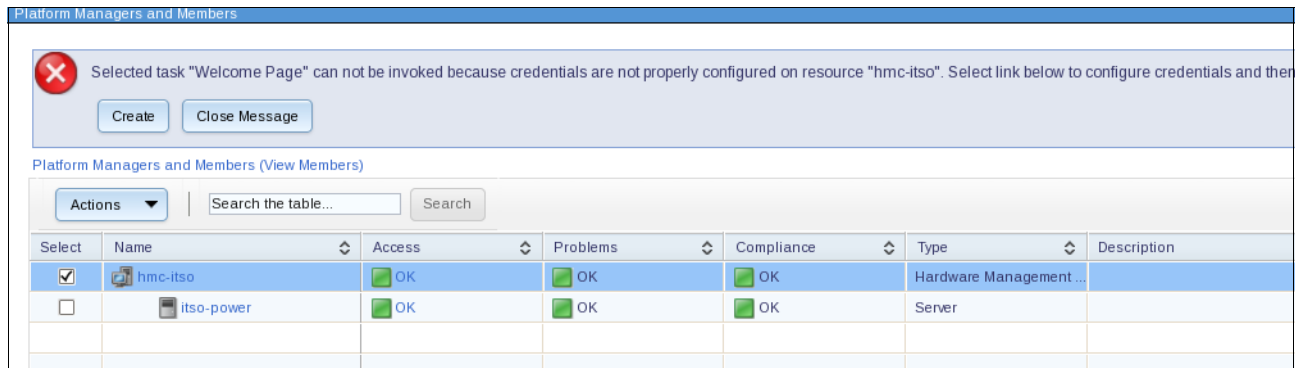


Figure 3-6 Configure SSO

9. Click **Create**. The Welcome wizard opens to enter valid SSO credentials (Figure 3-7).

The screenshot shows a web-based wizard titled "Create and Edit Single Sign-on Credentials". The left sidebar contains a navigation menu with three items: "Welcome" (checked), "Create Single Sign-on Credential" (highlighted with a blue arrow), and "Assign to IBM® Systems Director User". The main content area is titled "Create Single Sign-on Credential" and includes the instruction "Enter a valid user ID and password for system hmc-itso". Below this, there is a dropdown menu for "Authentication registry type:" set to "Local OS". Three input fields are provided: "*User ID:", "*Password:", and "*Verify password:", each with a corresponding text box.

Figure 3-7 Create and edit SSO

10. Enter a user ID and password. Then, click **Next**.

11. Assign to the IBM Systems Director User as shown in Figure 3-8.

The screenshot shows the next step in the wizard, titled "Assign to IBM® Systems Director User". The left sidebar now has "Assign to IBM® Systems Director User" highlighted with a blue arrow. The main content area has the instruction "Assign the previously created credentials to a known IBM® Systems Director user." Below this, there are two radio button options: "Use current user - root" (which is selected) and "Choose a different user". A table below lists available users:

Select	Name	Registry Type : Name	Type
<input type="radio"/>	root	Local OS : itso-aix00.itso.ibm.com	User ID and Password

At the bottom of the table, there is a pagination control showing "Page 1 of 1" and "Selected: 0 Total: 1".

Figure 3-8 Assign to IBM Systems Director User

12. At the end of the wizard, click **Finish**.

13. Because the SSO for the HMC that you selected is configured, reattempt Launch-in-Context (Figure 3-5 on page 123). The HMC does not launch and you are brought to the requested page (Figure 3-9).

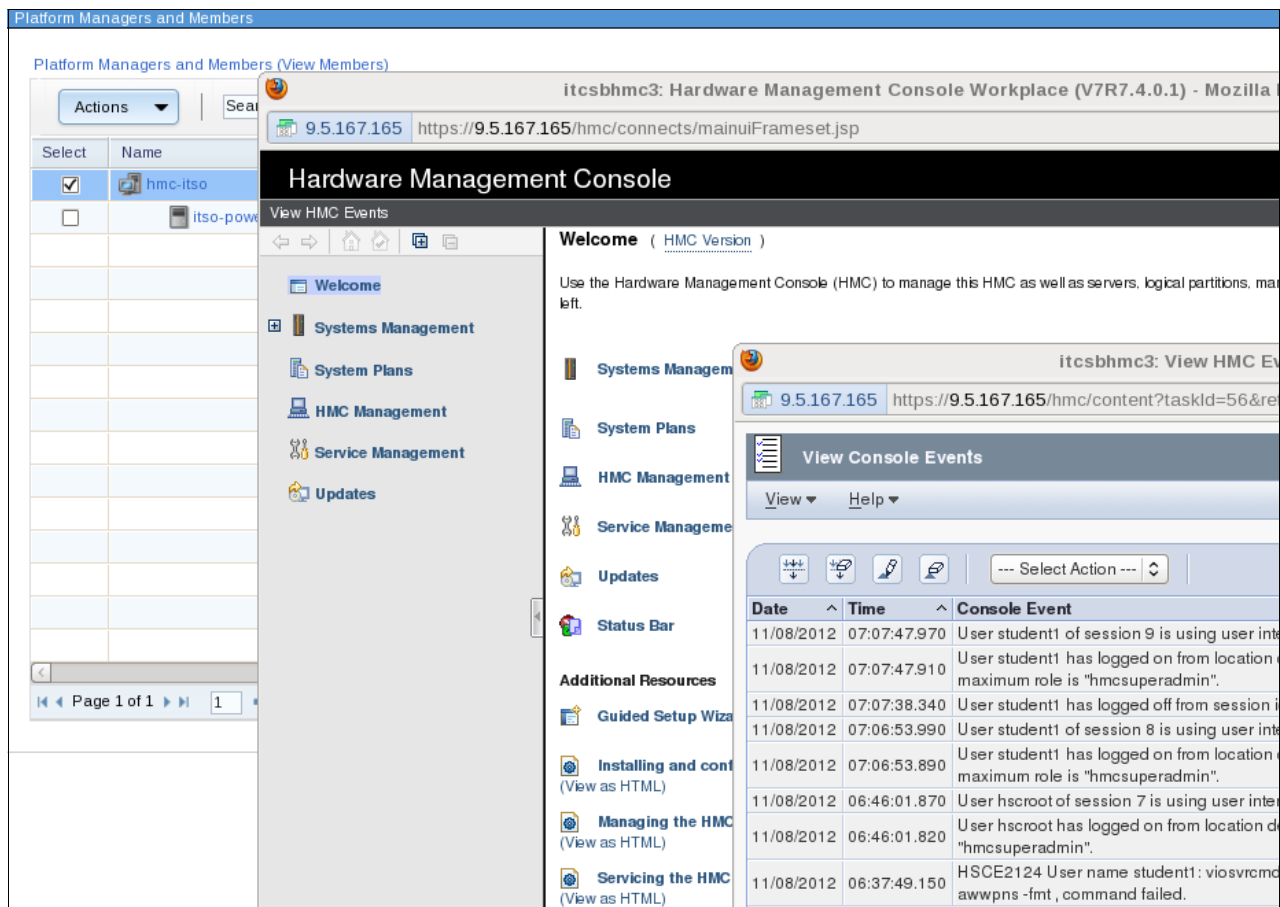


Figure 3-9 View Console Events

You can create a partition from the UI in two ways:

- ▶ Use LiC and launch the HMC UI (Figure 3-10 on page 126)
- ▶ Use the embedded view from the UI (Figure 3-12 on page 128)

By using LiC, you can also label the profile and assign these properties:

- ▶ Minimum processing units and memory
- ▶ Processing units and memory that you want
- ▶ Maximum processing units and memory
- ▶ Weighting for processing units

By using the standard LiC functionality, you can add virtual adapters while you build the virtual server. Depending on the complexity of the virtual server that you create, LiC gives you greater choice.

To create a virtual server by using LiC, follow these steps:

1. Right-click the server and click **Extended Management** → **Configuration** → **Create Logical Partition**. You can select to create an AIX or Linux partition, or an IBM i partition as shown in Figure 3-10.

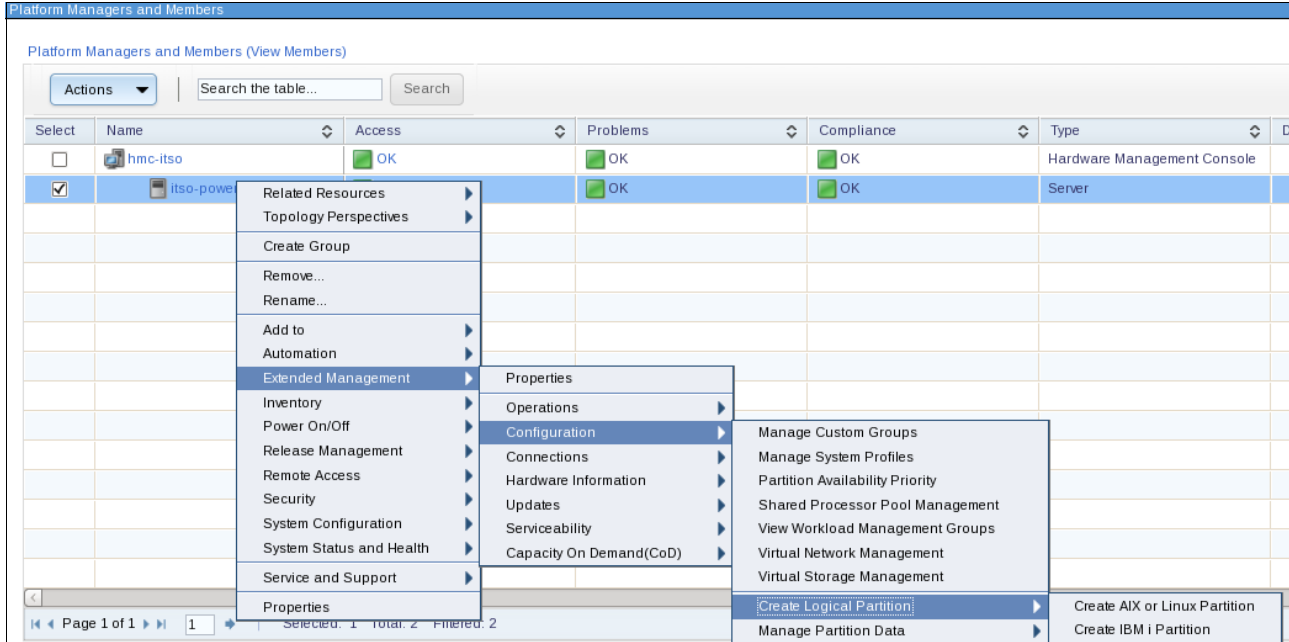


Figure 3-10 LiC virtual server creation

2. The HMC wizard opens in context (Figure 3-11).

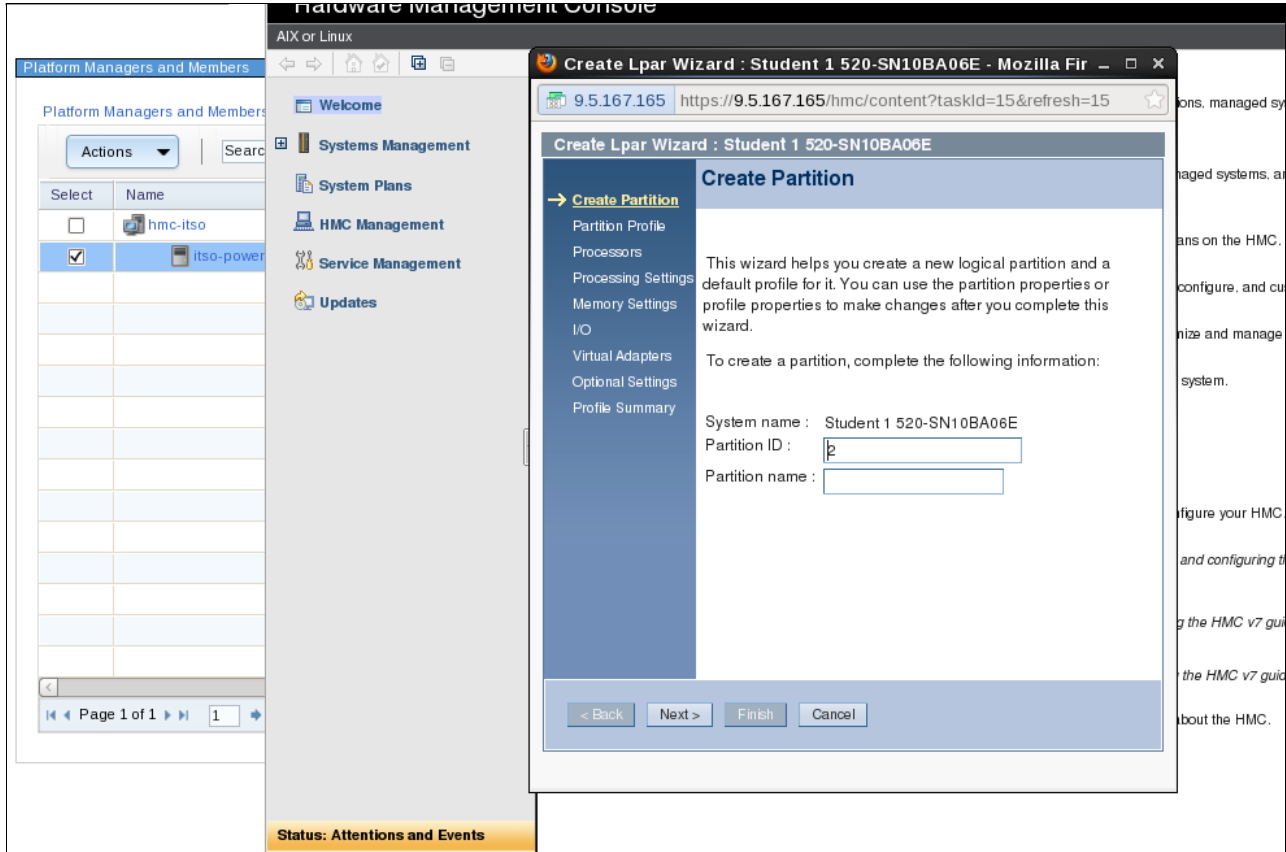


Figure 3-11 HMC LiC

Using the embedded menu simplifies the creation of the virtual server because you do not leave the UI as shown in Figure 3-12. Follow these steps:

1. Right-click the server and click **System Configuration** → **Create Virtual Server**.

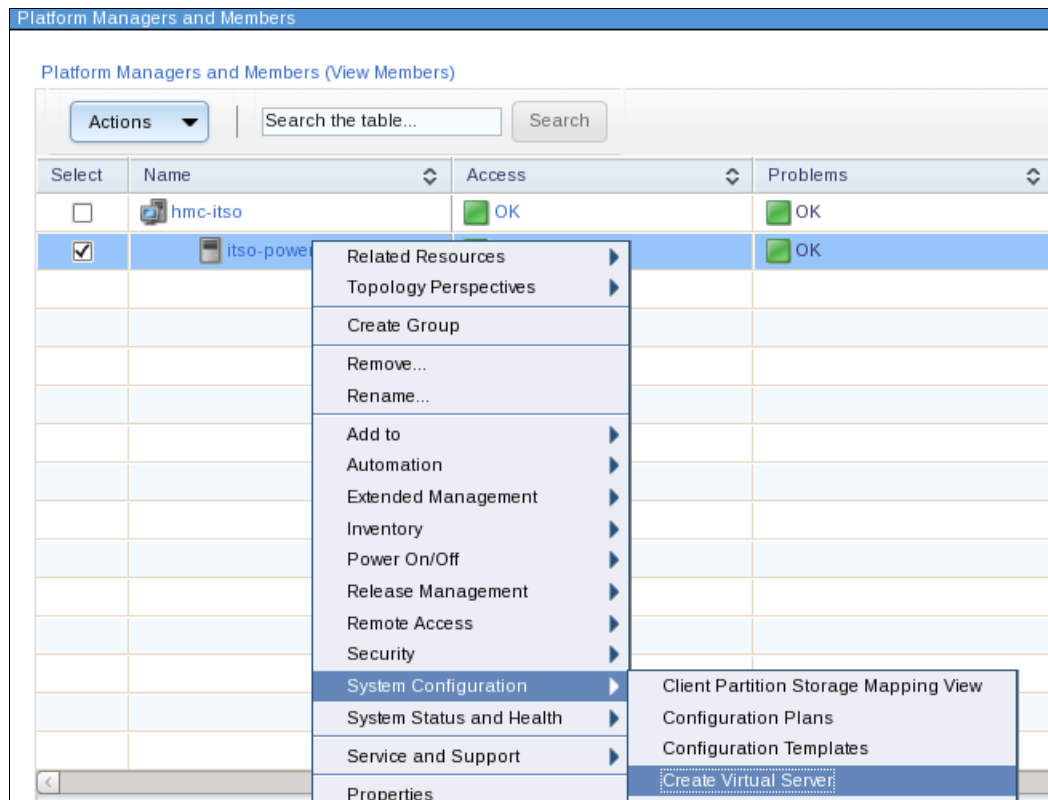


Figure 3-12 Virtual Server creation embedded

2. The Create Virtual Server wizard starts. In Figure 3-13, specify properties, such as name and source (AIX/Linux and processor).

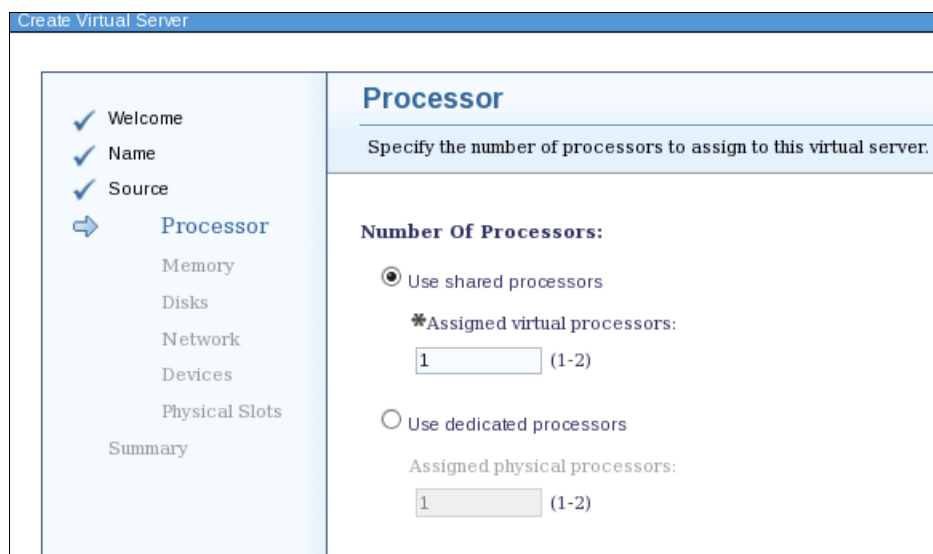


Figure 3-13 Create Virtual Server wizard

- Specify the memory size as required as shown in Figure 3-14.

Figure 3-14 Memory

- Disks depend on storage visibility or whether disks are already mapped to the Virtual I/O Server (VIOS) (Figure 3-15). Disks can be virtual or physical system service processors (SSPs) or N-Port ID Virtualization (NPIV) volumes.

Figure 3-15 Disks

- Network definitions are shown in Figure 3-16.

Select	Logical Network	Bridged	VLAN ID	Deployment State
<input checked="" type="checkbox"/>	Discovered/1/0	Yes	1	Existing on host

Figure 3-16 Networks

- For devices, use the normal practices that you use for a regular HMC LPAR creation (Figure 3-17).

Select	Name	State	Access	Problems	Compliance	OS Type an...
<input type="checkbox"/>	itso-power	Started	OK	OK	OK	
<input type="checkbox"/>	itso-ax00	Started	OK	OK	OK	AIX 6.1
<input type="checkbox"/>	itso-ax01	Started	OK	OK	OK	
<input type="checkbox"/>	itso-ax99	Stopped	OK	OK	OK	
<input type="checkbox"/>	itso-vio	Started	OK	OK	OK	VIOS 2.2.1.4

Figure 3-17 itso-ax99 completed

7. After the creation of a virtual server, additional networks can be added and CPU priority can be changed (Figure 3-18). Use this syntax:

```
smcli chvs -A "networks=+Discovered-XX-0" -n itso-aix99
```

```
# smcli chvs -A "cpupriority=128" -n itso-aix99
Edit virtual server operation completed successfully.
```

Figure 3-18 chvs cpupriority

8. You can increase or decrease memory within the virtual server minimum and maximum range (Figure 3-19 and Figure 3-20).

```
# smcli chvs -A "memsize=8192" itso-aix00
Edit virtual server operation completed successfully.
#
```

Figure 3-19 chvs memsize

```
# while true
> do
> lsattr -El sys0 -a realmem
> sleep 2
> done
realmem 7340032 Amount of usable physical memory in Kbytes False
realmem 7340032 Amount of usable physical memory in Kbytes False
realmem 7340032 Amount of usable physical memory in Kbytes False
realmem 8388608 Amount of usable physical memory in Kbytes False
realmem 8388608 Amount of usable physical memory in Kbytes False
```

Figure 3-20 chvs memsize output

- Memory, processor, and priority can be changed from the UI dynamically one time within the virtual server minimum and maximum range (Figure 3-21).

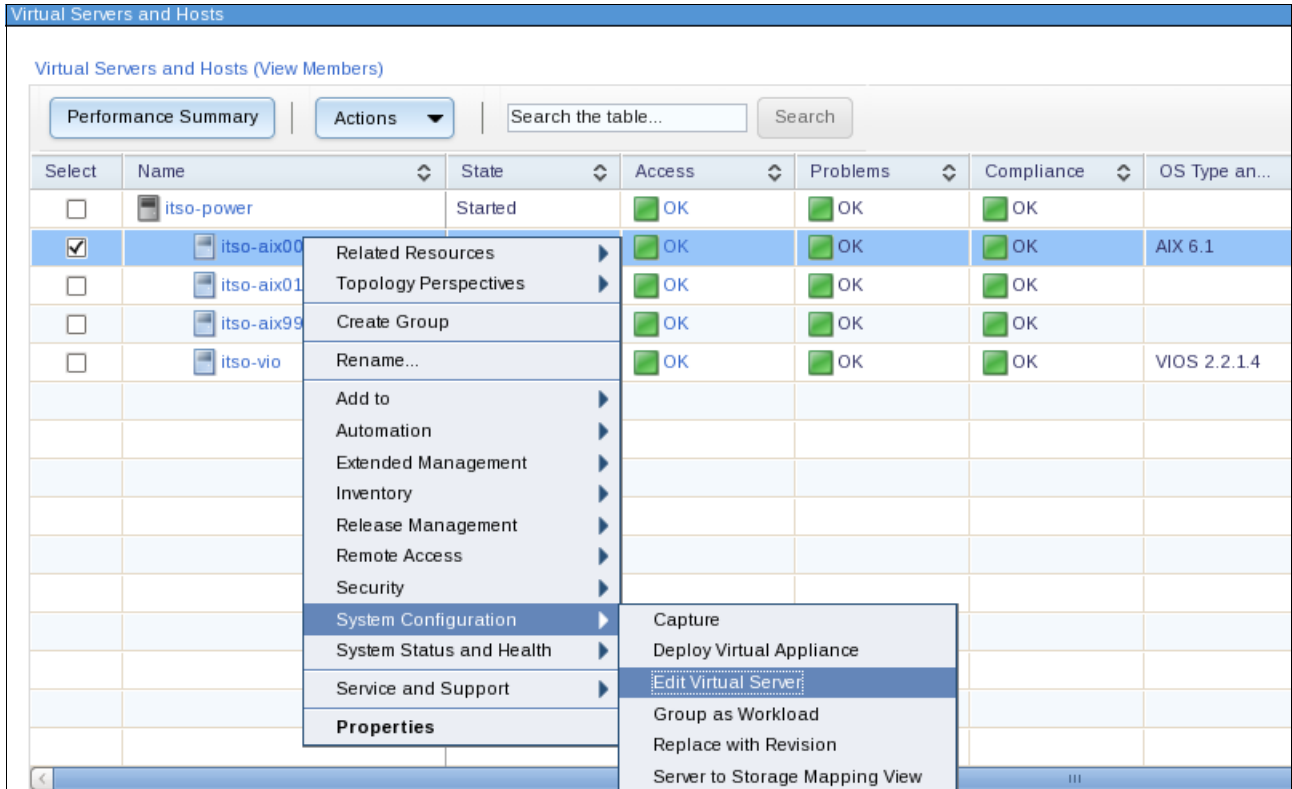


Figure 3-21 Edit Virtual Server option

10. Select the required tab and change the Assigned value (Figure 3-22). Click **OK**.

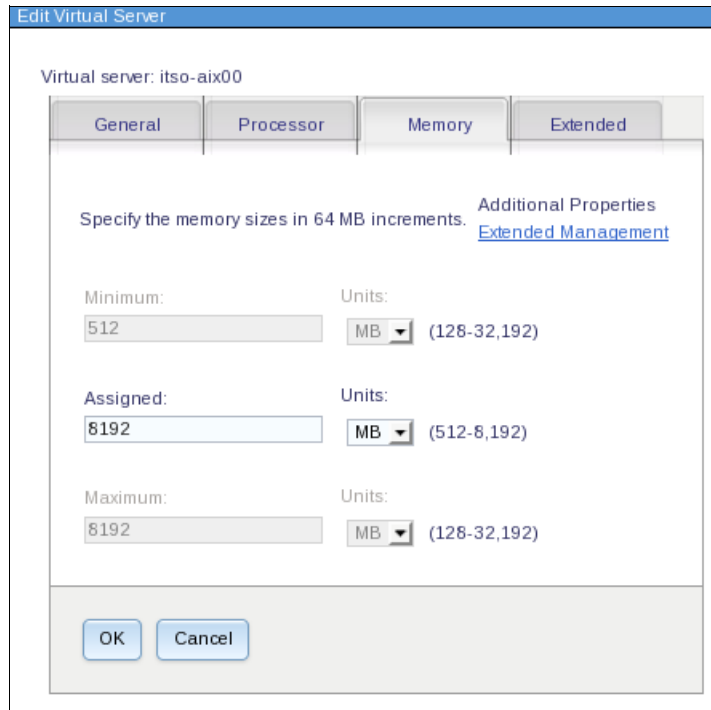


Figure 3-22 Edit virtual server memory

11. On the submitted job, click **Display Properties**. Click **Complete (view log)** to view the output of the job. See Figure 3-23.

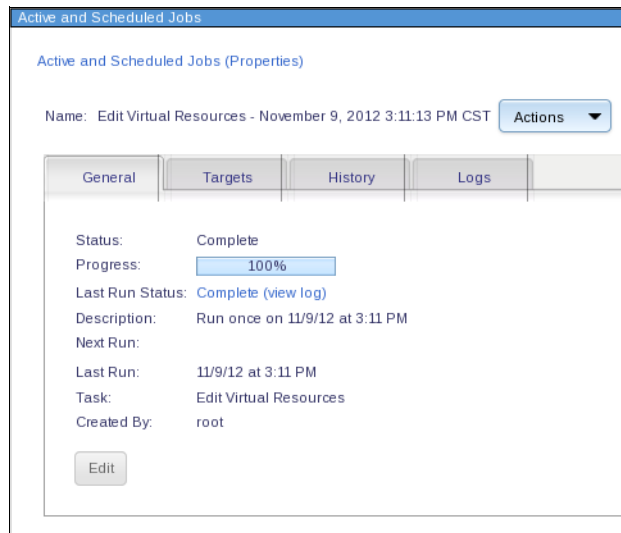


Figure 3-23 Job properties

12. Figure 3-24 shows the virtual server job output.

Active and Scheduled Jobs

Edit Virtual Resources - November 9, 2012 3:11:13 PM CST (Properties)

Name: Edit Virtual Resources - November 9, 2012 3:11:13 PM CST Actions

General | Targets | History | Logs

Click on job instance in the Name column in order to view its logs

Job Instance

Actions | Search the table... | Search

Select	Name	Status
<input checked="" type="checkbox"/>	11/9/12 at 3:11 PM	Complete

Page 1 of 1 | 1 | Selected: 1 Total: 1 Filtered: 1

Job log Message filter: All

```

November 9, 2012 3:11:30 PM CST-Level:1-MEID:0--MSG: Job "Edit Virtual Resources - November 9, 2012 3:11:13 PM CST" activated.
November 9, 2012 3:11:30 PM CST-Level:200-MEID:0--MSG: Subtask "Edit Virtual Resources" activated.
November 9, 2012 3:11:30 PM CST-Level:200-MEID:0--MSG: Starting clients
November 9, 2012 3:11:30 PM CST-Level:100-MEID:0--MSG: Clients started for task "Edit Virtual Resources"
November 9, 2012 3:11:30 PM CST-Level:200-MEID:0--MSG: Subtask activation status changed to "Active".
November 9, 2012 3:11:30 PM CST-Level:1-MEID:0--MSG: Job activation status changed to "Active".
November 9, 2012 3:11:30 PM CST-Level:50-MEID:3210--MSG: DNZVMP505I Edit Virtual Resources request started for virtual server, itso-aix00.
November 9, 2012 3:11:40 PM CST-Level:50-MEID:3210--MSG: DNZVMP500I Memory allocations have been updated on the managed resource.
November 9, 2012 3:11:44 PM CST-Level:50-MEID:3210--MSG: DNZVMP501I Processor allocations have been updated on the managed resource.
November 9, 2012 3:11:45 PM CST-Level:50-MEID:3210--MSG: DNZVMP506I Edit Virtual Resources request completed successfully for virtual server, itso-aix00.
November 9, 2012 3:11:45 PM CST-Level:100-MEID:3210--MSG: itso-aix00 client job status changed to "Complete".
November 9, 2012 3:11:45 PM CST-Level:200-MEID:0--MSG: Subtask activation status changed to "Complete".
November 9, 2012 3:11:45 PM CST-Level:1-MEID:0--MSG: Job activation status changed to "Complete".
    
```

Figure 3-24 Edit virtual server job output

13. Under the Systems Director UI, the **Inventory** → **Views** → **Virtual Servers and Hosts** view displays the changed memory value (Figure 3-25).

Virtual Servers and Hosts

Virtual Servers and Hosts (View Members)

Performance Summary | Actions | Search the table... | Search

Select	Name	State	Access	Problems	Memory (MB)	Processors
<input type="checkbox"/>	itso-power	Started	OK	OK	32,768	
<input checked="" type="checkbox"/>	itso-aix00	Started	OK	OK	8,192	

Figure 3-25 Updated server configuration

3.2 Light path diagnostics

IBM x86 servers provide a diagnostic tool called *light path diagnostics* (LPDs) as an easy way to find hardware problems on the systems when they occur. LPDs consist of three components:

- ▶ A system warning LED on the front of the server.
- ▶ A panel of LEDs in a pop-out panel (or a panel inside or outside the server for some systems). This panel shows the status of major subsystems, for example, memory.
- ▶ Individual LEDs beside each component in the system, for example, each memory dual inline memory module (DIMM).

For information about the LPD LEDs that are available on your System x, BladeCenter, or Flex System hardware, see the server documentation.

The Systems Director can read this LPD information. This information is provided by the service processors that are integrated in the server:

- ▶ Integrated Management Module (IMM)
- ▶ IMMv2
- ▶ Advanced Management Module (AMM)
- ▶ Chassis Management Module (CMM)

You can view LPD status information from the Systems Director UI or the command-line interface (CLI).

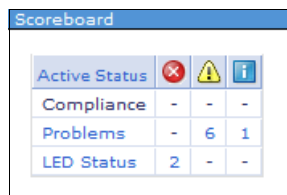
There are multiple ways to select the detailed LPD information:

- ▶ From the health summary, click **LED status** in the scoreboard.
- ▶ From the Resource Explorer window, in the LED Status column, click the red, yellow, or blue icon.
- ▶ From the right-click menu of a system, click **System status and health** → **Lightpath**.
- ▶ From a command-line prompt, use the command `smcli lsled`.

We describe each way.

3.2.1 LED status in the scoreboard

On the home page of Systems Director, the health summary scorecard shows a summary of systems with LPD alerts under the name LED Status. Figure 3-26 shows an example.



The screenshot shows a 'Scoreboard' window with a table of system metrics. The 'LED Status' row shows 2 active alerts, 0 warnings, and 0 informational messages.

Active Status	✖	⚠	i
Compliance	-	-	-
Problems	-	6	1
LED Status	2	-	-

Figure 3-26 Scoreboard that shows the LED status

When you click **LED Status**, a window opens that shows systems with alerts as shown in Figure 3-27.

Navigate Resources

Resources with Critical Problems

Actions | Search the table... Search

Select	Name	Access	LED Status
<input type="checkbox"/>	BCS-aMM-FFM	OK	Critical
<input type="checkbox"/>	IBM BC H	OK	Critical

Figure 3-27 Systems with problems

If you click the LED status of the individual systems, you see the specific alert details as reported by the SSP as shown in Figure 3-28.

Lightpath

View the status of each LED on the target system.

BCS-aMM-FFM | Browse...

BCS-aMM-FFM (Lightpath Diagnostics)

Verify LED Status | Actions | Search the table... Search

Select	LED Name	LED State	LED Color	Indicated Condi...	LED Locatio
<input type="checkbox"/>	Fault	On	Orange	Attention	FrontPanel
<input type="checkbox"/>	Information	On	Orange		FrontPanel
<input type="checkbox"/>	Location	Off	Blue	Location	FrontPanel
<input type="checkbox"/>	Over Temp	Off	Orange	Fault	FrontPanel

Figure 3-28 Light-path detailed view

3.2.2 LED status in the Resource Explorer

To view the LPD status and information, first add a column for LED status to the Resource Explorer view for a group. When you are in a group in the Resource Explorer windows, click **Actions** → **Columns** as shown in Figure 3-29.

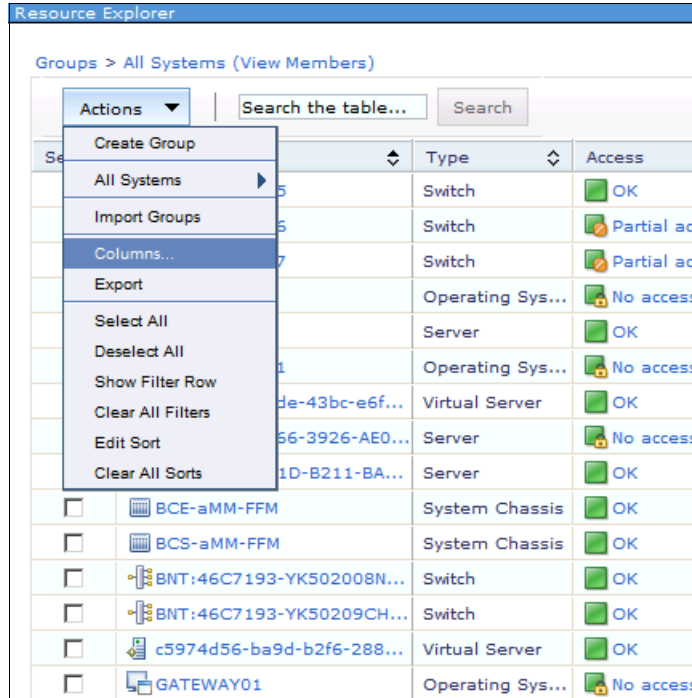


Figure 3-29 Select to add columns to the group view

In Figure 3-30, select **LED Status** from the Available Columns list on the left. Click **Add** to add LED Status to the Selected Columns list. Use **Up** and **Down** to change the relative position of the column. Click **OK** to save the changes. See Figure 3-30.

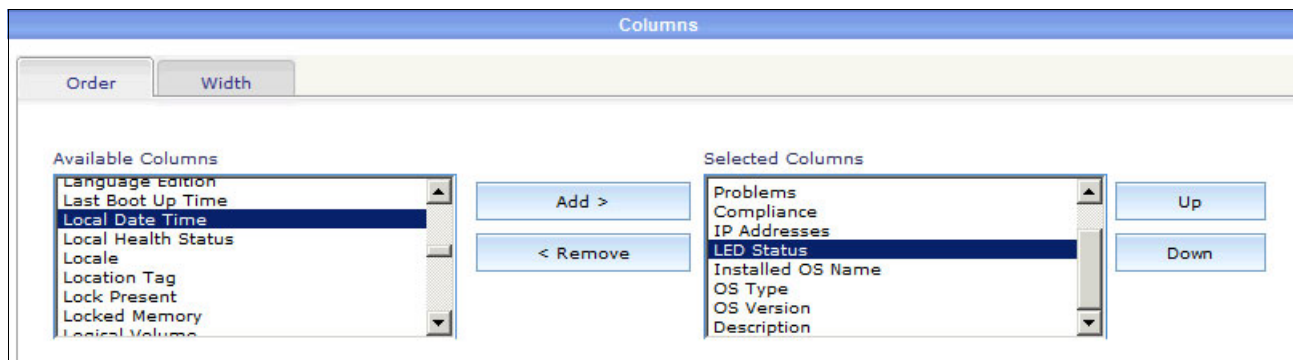


Figure 3-30 Select LED Status to add a column to the Resource Explorer view

Now, the new LED Status column is displayed in the Resource Explorer window as shown in Figure 3-31.

Resource Explorer

Groups > All Systems (View Members)

Actions | Search the table... Search

Select	Name	Type	Access	Pro...	Co...	IP Addresses	LED Status
<input type="checkbox"/>	192.168.15.15	Switch	OK	Info...	OK	192.168.15.15	OK
<input type="checkbox"/>	192.168.15.16	Switch	Partial...	OK	OK	192.168.15.16	OK
<input type="checkbox"/>	192.168.15.17	Switch	Partial...	OK	OK	192.168.15.17	OK
<input type="checkbox"/>	192.168.15.2	Operating Sys...	No acc...	OK	OK	192.168.15.2	OK
<input type="checkbox"/>	192.168.15.3	Server	OK	OK	OK	fe80:0:0:3640:b...	OK
<input type="checkbox"/>	192.168.15.61	Operating Sys...	No acc...	OK	OK	192.168.15.61	OK
<input type="checkbox"/>	5d224d56-03de-43bc-e6f...	Virtual Server	OK	OK	OK	10.13.9.2, 192.16...	OK
<input type="checkbox"/>	B10E9C1A-7566-3926-AE0...	Server	No acc...	OK	OK	192.168.15.81	OK
<input type="checkbox"/>	BC1DE63D-EA1D-B211-BA...	Server	OK	OK	OK		OK
<input type="checkbox"/>	BCE-aMM-FFM	System Chassis	OK	OK	OK	192.168.15.100, f...	OK
<input type="checkbox"/>	BCS-aMM-FFM	System Chassis	OK	OK	OK	192.168.15.105, f...	Critical
<input type="checkbox"/>	BNT:46C7193-YK502008N...	Switch	OK	War...	OK	192.168.15.122	OK
<input type="checkbox"/>	BNT:46C7193-YK50209CH...	Switch	OK	War...	OK	192.168.15.124	OK
<input type="checkbox"/>	c5974d56-ba9d-b2f6-288...	Virtual Server	OK	OK	OK	2001:0:5ef5:79fb:...	OK
<input type="checkbox"/>	GATEWAY01	Operating Sys...	No acc...	OK	OK	192.168.15.1	OK

Page 1 of 4 | 1 | Selected: 0 Total: 51 Filtered: 51

Figure 3-31 LED Status column in Resource Explorer

If a critical, warning, or informational status message from a managed system exists on the LPD panel, you see the status. The status displays as a red, yellow, or blue icon in the LED Status column. See Figure 3-31.

After you add the column, you can click the status to see the detailed view (Figure 3-28 on page 135).

3.2.3 LED Status from the menu of a system

To see the LED status and detailed information for a single system, right-click the system and click **System Status and Health** → **Lightpath**. See Figure 3-32. The window that opens is similar to the window from our example in Figure 3-28 on page 135.

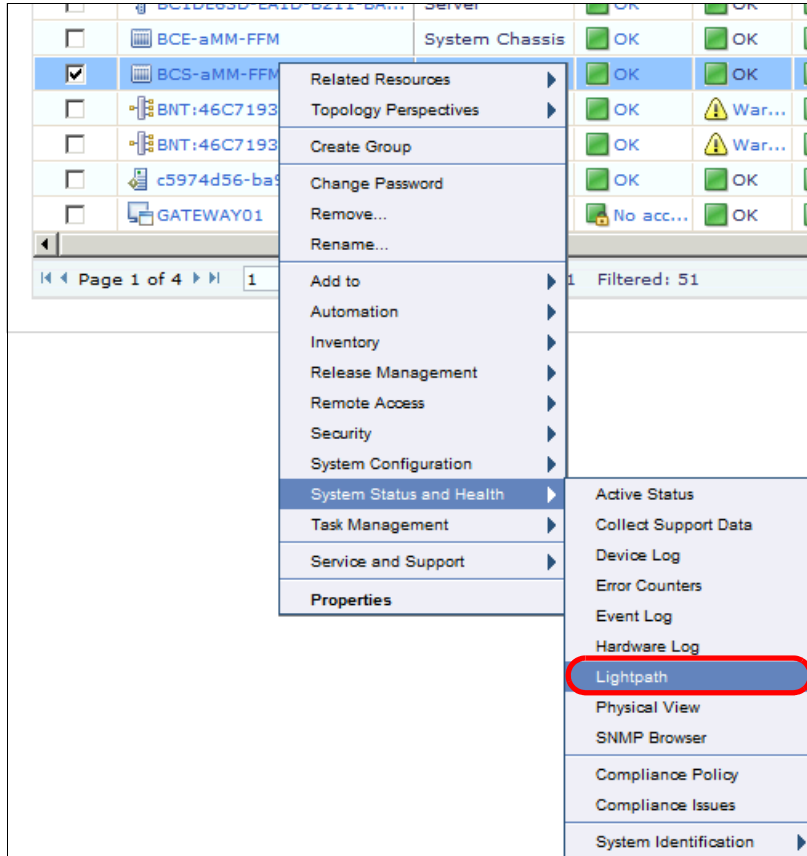


Figure 3-32 Lightpath menu for single system

3.2.4 SMCLI command-line interface

You can also use the `smcli lsled` CLI command to see the LED status for a system. The results of our example are shown in Example 3-1.

Example 3-1 smcli lsled

```
PS C:\Windows\system32> smcli lsled -s all -i 9.42.171.73
-----
System Name: BC5AMM-----
Name          State      Color      Location
-----
Over Temp     Off        Orange     FrontPanel
Information    On         Orange     FrontPanel
Location      Off        Blue       FrontPanel
Fault         On         Orange     FrontPanel
-----
```


Example 3-1 on page 138 is the output from the command for a BladeCenter chassis that shows the status of all LEDs. This output shows that the Information and Fault LEDs for this system are on. The output also shows that the LEDs are on the front panel of the system.

If you want to see only the LEDs that are on or flashing, use the `-s all`, `-s on`, or `-s flash` option for this command. Or, use `-s on, flash` to see all LEDs that are on and blinking. In our example, we use the following command to make the LED on a remote server blink:

```
smcli runtask -i 9.42.171.173 "LED Flash"
```

Then, we run the `smcli lsled` command with the `-s flash` option again. Example 3-2 shows the result.

Example 3-2 smcli lsled -s flash

```
PS C:\Windows\system32> smcli lsled -s flash -i 9.42.171.73
```

```
-----  
System Name: BC5AMM-----
```

Name	State	Color	Location
Location	Blinking	Blue	FrontPanel

For detailed information about the options for the `smcli lsled` command, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_lsled.html

3.3 Hardware logs

Hardware log information is provided by the service processors from the systems. The following service processors and management modules provide the hardware log information to the Systems Director:

- ▶ Baseboard management controller (BMC)
- ▶ Remote Supervisor Adapter II (RSA II)
- ▶ Remote Supervisor Adapter (RSA)
- ▶ Management Module (MM)
- ▶ Integrated Management Module (IMMv1 and IMMv2)
- ▶ Advanced Management Module (AMM)
- ▶ Chassis Management Module (CMM)

Power Systems: LPD information for Power Systems is not accessible, except for IBM POWER® based servers in the BladeCenter and Flex System.

The information is provided by using an inband communication or out-of-band communication. The access path depends on the system hardware and configuration.

See Table 3-1.

Table 3-1 Service Processor hardware log access path

Systems	Service Processor	Hardware log access path
BladeCenter	Management Module (MM)	Out-of-band communication
BladeCenter	Advanced Management Module (AMM)	Out-of-band communication
Flex System	Chassis Management Module (CMM)	Out-of-band communication, only if no Flex System Manager (FSM) is installed and used
System x	Remote Supervisor Adapter (RSA)	Out-of-band communication
System x	Remote Supervisor Adapter II (RSAll)	Out-of-band communication
System x BladeCenter	Baseboard Management Controller (BMC)	Out-of-band communication. Inband communication that uses Common Agent or Platform Agent
System x	Integrated Management Module (IMMv1 or IMMv2 in rack or tower server)	Out-of-band communication. Inband communication that uses Common Agent or Platform Agent
BladeCenter Flex System	Flex System and BladeCenter Integrated Management Module (IMMv1 or IMMv2) in server	Out-of-band communication over AMM/CMM only. Inband communication that uses Common Agent or Platform Agent

Inband communication means that Systems Director accesses the agent on the system. This agent can read the hardware log information from the service processor (RSA, RSAll, IMM, IMMv2, or BMC) of the system. The agent uses a driver or other communication channels inside the system.

Out-of-band communication means that a direct connection exists from the Systems Director to the service processor over a TCP/IP communication. This communication is independent from the system state (power on/off). This communication is also independent from the operating system (running, starting, stopped). The minimum requirement is that the system has power and the Systems Director can access the service processor.

To access the hardware log information inband, you must have full access to the system and the system must be online. If you obtain the hardware log out-of-band, you can also access it from the System x server when this server is powered off. In Table 3-2, you can see which resource you must select to access the hardware log information.

Table 3-2 Selection of system resource for accessing the hardware log

Option	Description
Inband communication	Select the system that represents the Common Agent or Platform Agent.
Out-of-band communication with a system	Click the system, then select service processors or select the server.
Out-of-band communication with a BladeCenter chassis	Select the chassis.

Follow these steps to access the log information:

1. From the Resource Explorer window, right-click the system and click **Systems Status and Health** → **Hardware Log** (Figure 3-33).

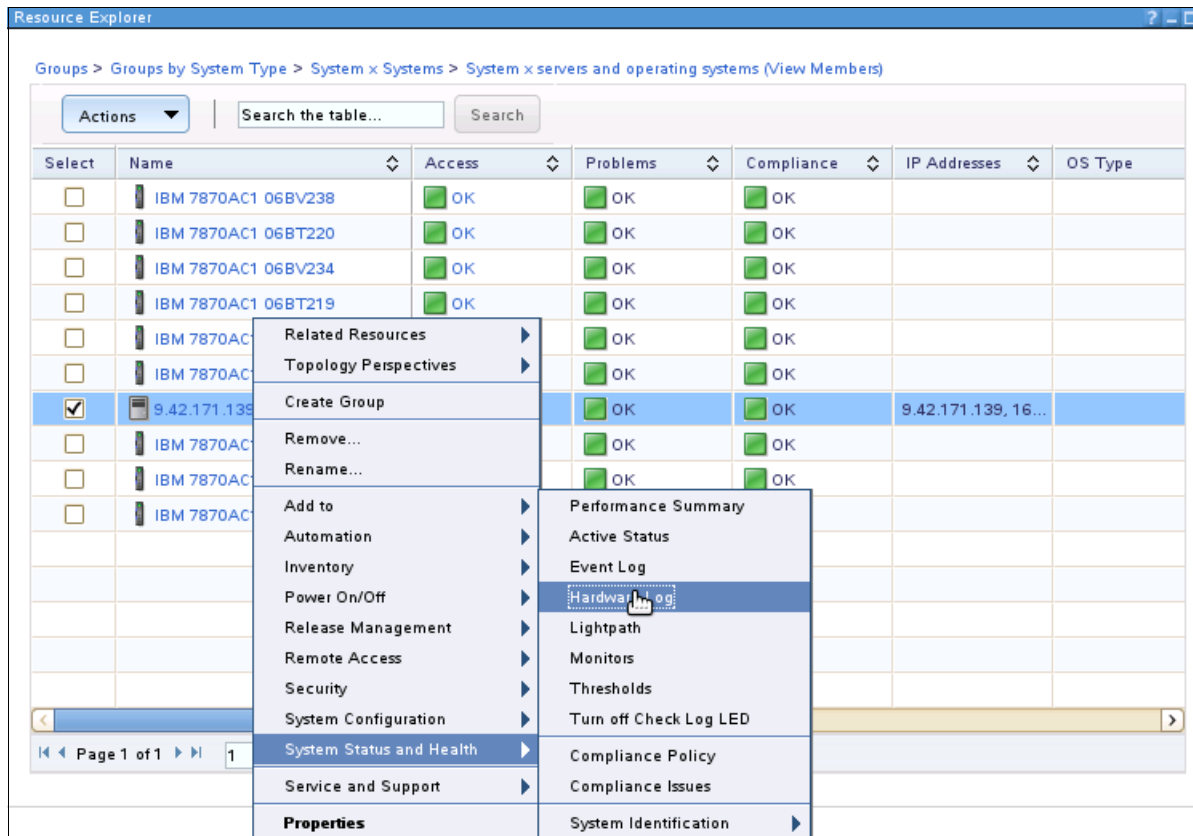


Figure 3-33 Select Hardware Log

- The window in Figure 3-34 opens to show the log entries that the Systems Director read from the service processor.

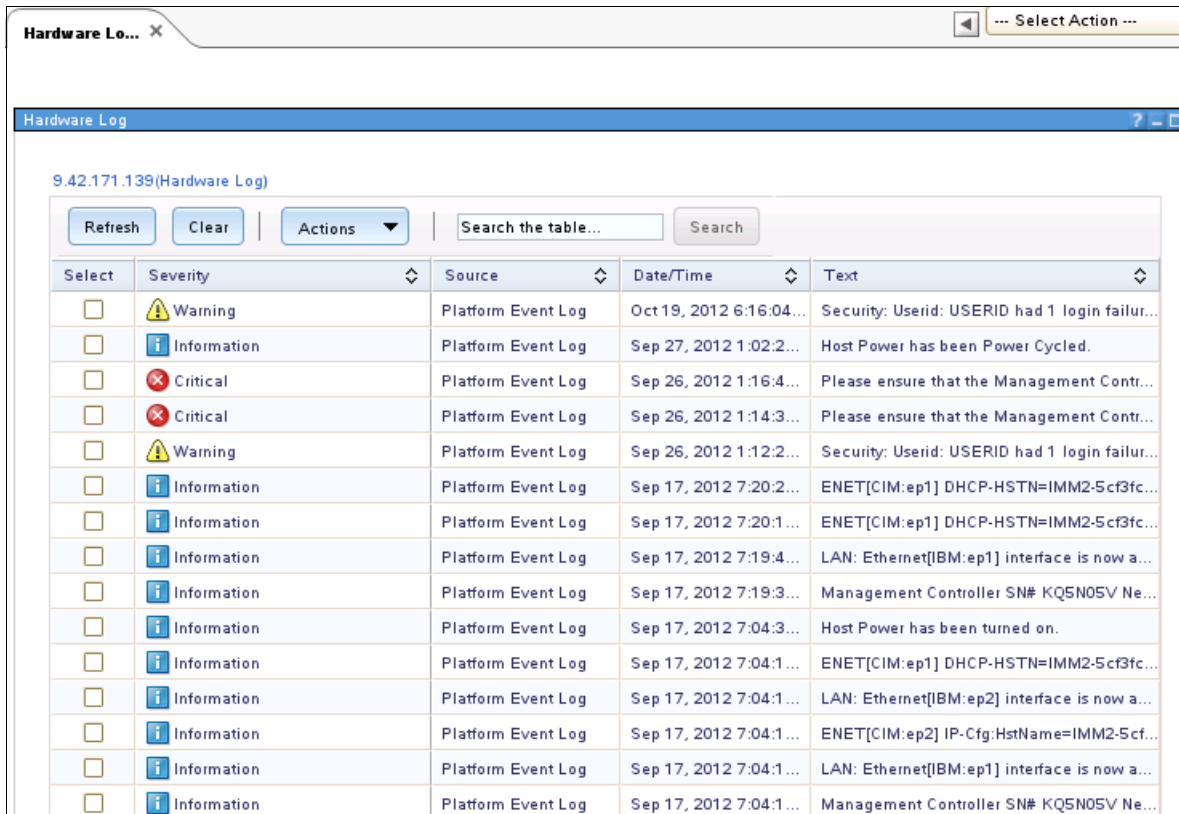


Figure 3-34 Hardware Log

- You can refresh the view, clear the entire log, or filter the view by using the Search function. You can also sort the view by clicking any of the column headings. From the Actions menu (Figure 3-35), you can export the log for problem determination. You can send the exported log information to IBM Support, if requested. The information is saved in CSV format.

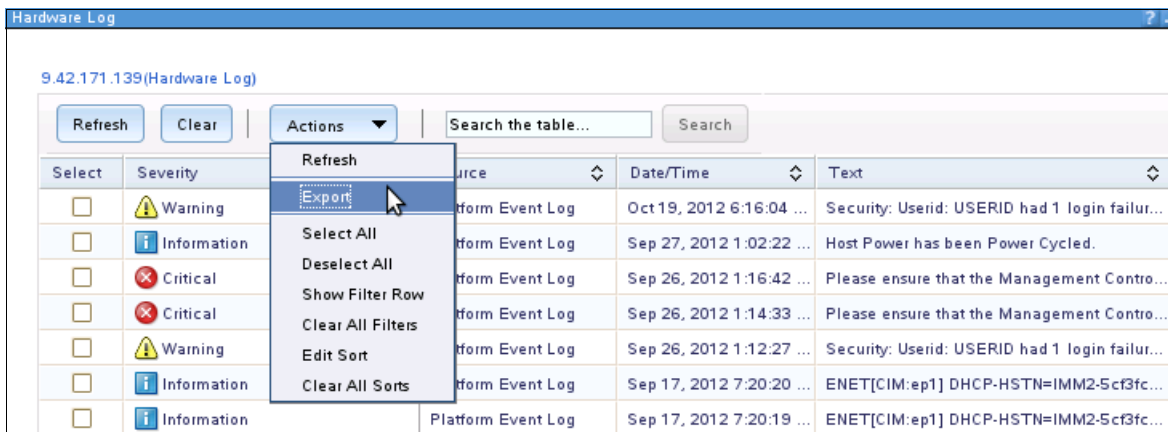


Figure 3-35 Save hardware log

3.4 Service and Support Manager

Service and Support Manager manages serviceable problems and reports the events to IBM. A *serviceable problem* is a problem to which IBM service typically responds, such as a failure of a hardware component that is under warranty.

Service and Support Manager is documented in the information center:

http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.esa.director.help/esa_kickoff.html

Service and Support Manager is viewed as an advanced manager within Systems Director, although it is installed with the base Systems Director server installation. The core objective of Service and Support Manager is to work with service information:

- ▶ Supported systems monitoring
- ▶ Serviceable event processing
- ▶ Support file management
- ▶ CLI support
- ▶ Collection of performance management data to send to IBM

The systems and resources that are eligible for monitoring by Service and Support Manager are listed in the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.esa.director.help%2Fesa_eligibility.html

Service and Support Manager subscribes to Systems Director events and filters out unserviceable events. When a serviceable event is received by Service and Support Manager, it submits a service request for the applicable event to IBM. Service and Support Manager runs data collectors on managed endpoints by using snap for AIX and Linux on Power Systems. Service and Support Manager runs data collectors on managed endpoints by using Dynamic System Analysis for Linux and Windows on IBM x86 systems.

To launch Service and Support Manager from the Systems Director home page, click **Plug-ins** and scroll down to **Service and Support Manager**.

The Service and Support Manager main page is shown in Figure 3-36.

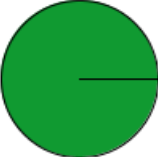
Service and Support Manager

Service and Support Manager

Manage serviceable problems on your systems.

Problem Reporting

Serviceable Problems for 1 Monitored Systems



⚠️ 0 systems with serviceable problems

✅ 1 system with no open serviceable problems

Electronic Services Links

- [Serviceable Problems](#)
- [All Problems](#)
- [IBM Support Portal](#)
- [Open a service request](#)

Recent Activity

- ⚠️ 0 serviceable problems require attention
- i 0 service requests being investigated by IBM
- i 0 requests have been updated in the last 24 hours
- i 0 serviceable problems opened in the last 24 hours

Status

⚠️ **Not activated.** Service and Support Manager is actively monitoring for serviceable problems. However, Electronic Service Agent™ is not configured for electronic service transmissions. Complete the Getting Started wizard to enable the transmission of problems, inventory, and performance measurement data to IBM.

⚠️ **Dynamic System Analysis (DSA) status error.** Service and Support Manager encountered a problem trying to verify the status of the DSA collectors. Electronic Service Agent™ has not been configured. Complete the Getting Started wizard, then try 'Test connection' task to verify connection to backend.

Common Tasks

- [Getting Started with Electronic Service Agent...](#)
- [Manage support files](#)
- [Verify DSA status](#)

Setup and Configuration

[Getting Started with Electronic Service Agent](#)

Figure 3-36 Service and Support Manager

144 IBM Systems Director 6.3 Best Practices: Installation and Configuration

Service and Support Manager creates default groups within Systems Director. The groups are under **Resource Explorer** → **Groups** → **Service and Support Groups** as shown in Figure 3-37. The groups are dynamic and automatically populated.

Select	Name	Type	Description
<input type="checkbox"/>	Excluded Systems (0)	Dynamic: System	Contains systems not eligible for Service and Support Manager
<input type="checkbox"/>	Monitored Systems (1)	Dynamic: System	Contains systems currently monitored by Service and Support Manager
<input type="checkbox"/>	Unknown Systems (0)	Dynamic: System	Contains systems not recognized by Service and Support Manager

Figure 3-37 Service and Support Manager groups

3.4.1 Connectivity to IBM

The message in the Status section in Figure 3-36 on page 144 shows that IBM Electronic Service Agent™ (ESA) needs to be configured. You use ESA for electronic transmissions to IBM. To configure ESA, click **Getting Started with Electronic Service Agent** under Setup and Configuration in Figure 3-36 on page 144.

The configuration is driven by a wizard and requires the following actions and input:

- ▶ Provide company contact and system location
- ▶ Configure connectivity to IBM:
 - Director Connection
 - Proxy Access
- ▶ Authorize an IBM ID

After you enter the required information, Service and Support Manager is ready as shown in Figure 3-38.

Status

✓ **Ready.** Service and Support Manager is actively monitoring for serviceable problems and Electronic Service Agent™ is configured to automatically transmit problems, inventory, and performance measurement data to IBM.

⚠ **Dynamic System Analysis (DSA) status error.** Service and Support Manager encountered a problem trying to verify the status of the DSA collectors. Please try 'Verify DSA status' task again or 'Test connection' task to verify connection to backend.

Common Tasks

- [Manage support files](#)
- [Send test problem](#)
- [Test connection to IBM](#)
- [Verify DSA status](#)

Figure 3-38 Electronic Service Agent Status

For Service and Support Manager to function, you need to enable connectivity through your firewall to IBM. The addresses and ports that are used are listed in Table 3-3.

Table 3-3 SSM proxy

Host name	IP address	Port
www6.software.ibm.com	207.25.253.41	443
	192.109.81.20	443
download2.boulder.ibm.com	207.25.253.8	80
download3.boulder.ibm.com	207.25.253.76	80
eccgw01.boulder.ibm.com	207.25.252.197	443
eccgw02.rochester.ibm.com	129.42.160.51	443
www-945.ibm.com	129.42.26.224 129.42.34.224 129.42.42.224	443
www.ibm.com	129.42.56.216 129.42.58.216 129.42.60.216	443 or 80
www-03.ibm.com	204.146.30.17	80

If you encounter problems, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.tbs.helps.doc/fqm0_r_tbs_um_proxy_issues.html

3.4.2 Enabling systems for service and support

Perform the following tasks to enable a system for monitoring:

- ▶ The system is discovered.
- ▶ The system is unlocked.
- ▶ An inventory is collected.

After the tasks are complete, check whether the ESA agent is running on your endpoints. For guidance, see this information center page:

http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.esa.director.help/esa_problem_optimize.html

To enable reporting to IBM, follow the steps in this information center page:

http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.esa.director.help/esa_enable_disable_problem.html

To check the functionality, send a test problem by using the **Send test problem link** in Common Tasks as shown in Figure 3-39.

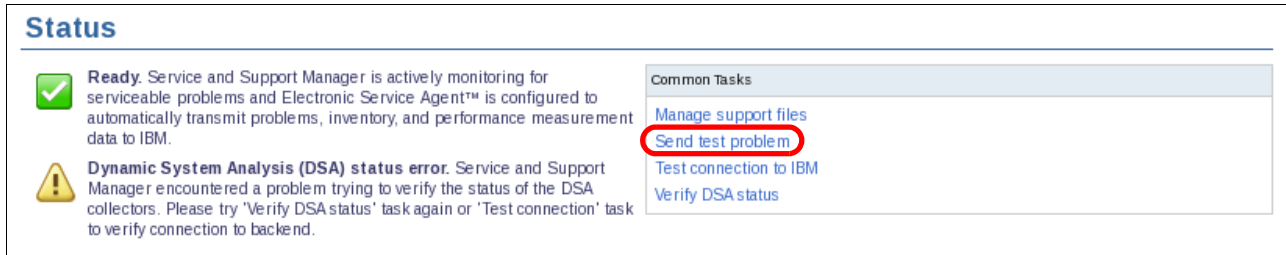


Figure 3-39 Electronic Service Agent Status

A reminder appears that this action sends an actual report to IBM Support (Figure 3-40).

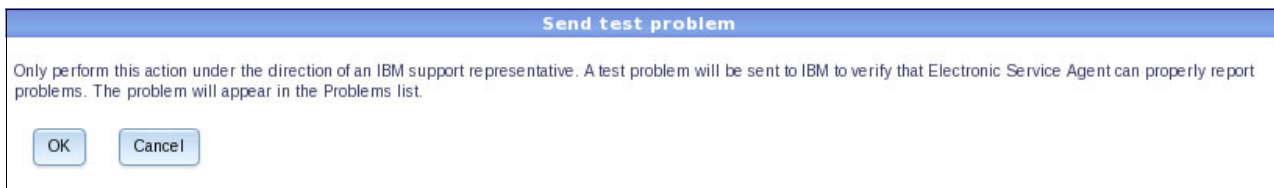


Figure 3-40 Send test problem confirmation

After you click **OK**, the test problem report is submitted to IBM Support. This report is visible under the dashboard and the Problem Reporting view (Figure 3-41).

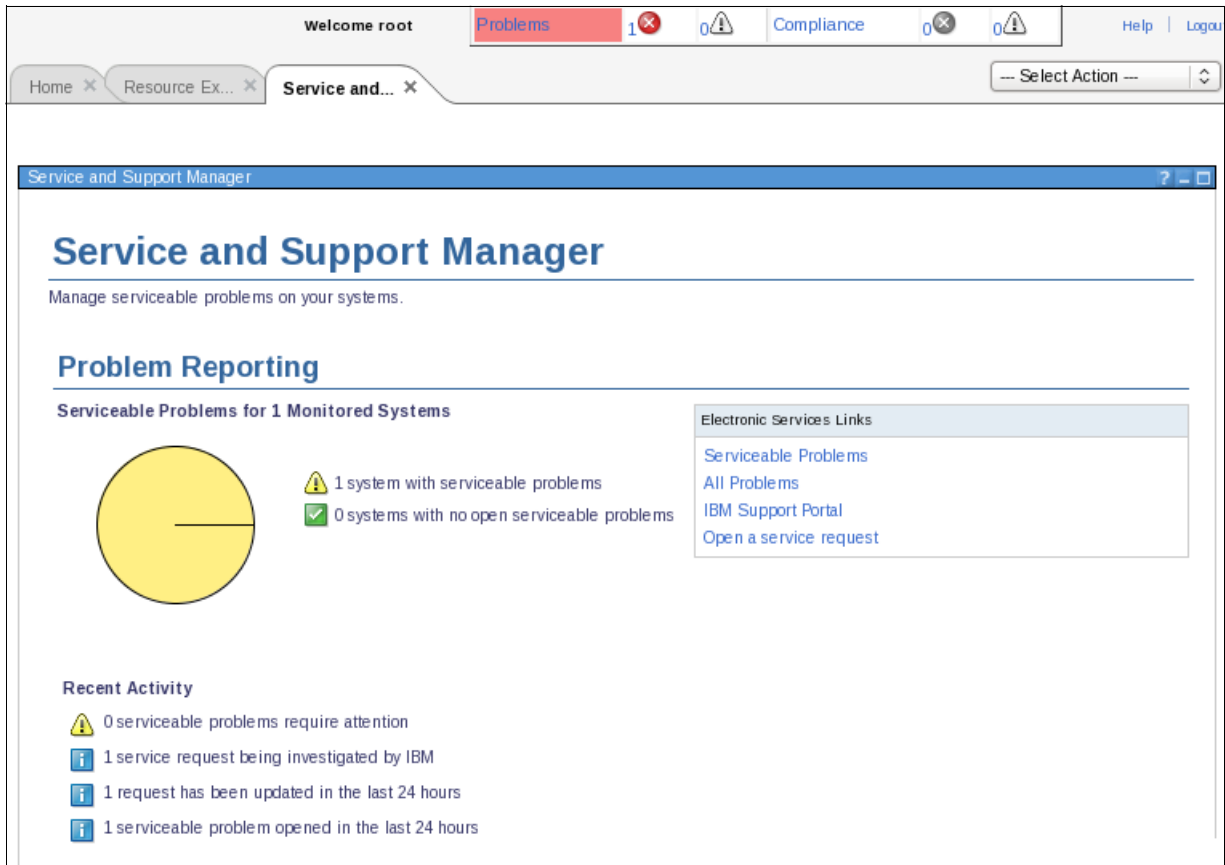


Figure 3-41 Service and Support Manager: Problem Reporting view

3.4.3 Serviceable event processing

Serviceable event processing is the management and transmission of serviceable events for hardware problems to IBM.

Serviceable events are determined by IBM and cannot be altered. The analysis component of Service and Support Manager determines whether the event warrants the creation of a serviceable event. Serviceable events are viewable in the Service and Support Manager plug-in as shown in Figure 3-41 on page 147.

If an event is serviceable and Service and Support Manager is fully configured, the service request is transferred automatically to IBM unless otherwise configured.

Duplicate event processing is supported. Any duplicate event that is generated within a 24-hour window does not generate a new ticket with IBM.

3.4.4 Managing support files

After the problem is submitted to IBM Support, additional data that is associated with the problem can be uploaded to IBM to help diagnose the problem. The data includes detailed system information, dump files, and event logs.

Follow these steps to view the support files and then submit them to IBM:

1. Under Common Tasks in the Service and Support Manager home page, Figure 3-36 on page 144, select **Manage Support Files**. The window that is shown in Figure 3-42 opens.

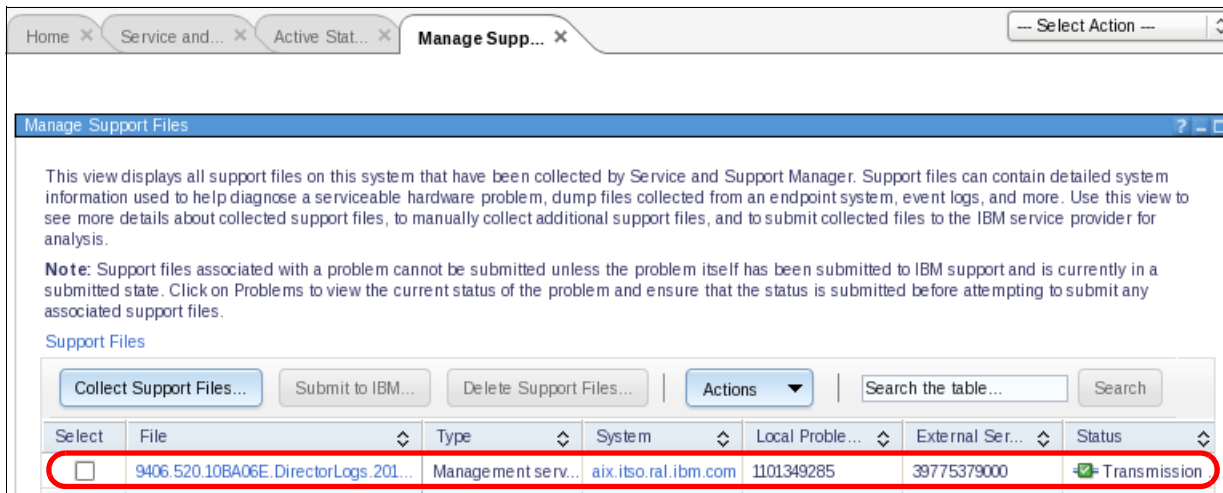


Figure 3-42 Manage Support Files

2. When you collect support files, select the monitored system where you want to collect the support files and click **Collect Support Files**. Use the predefined groups as listed in Figure 3-37 on page 145.

3. Choose the target system as shown in Figure 3-43.

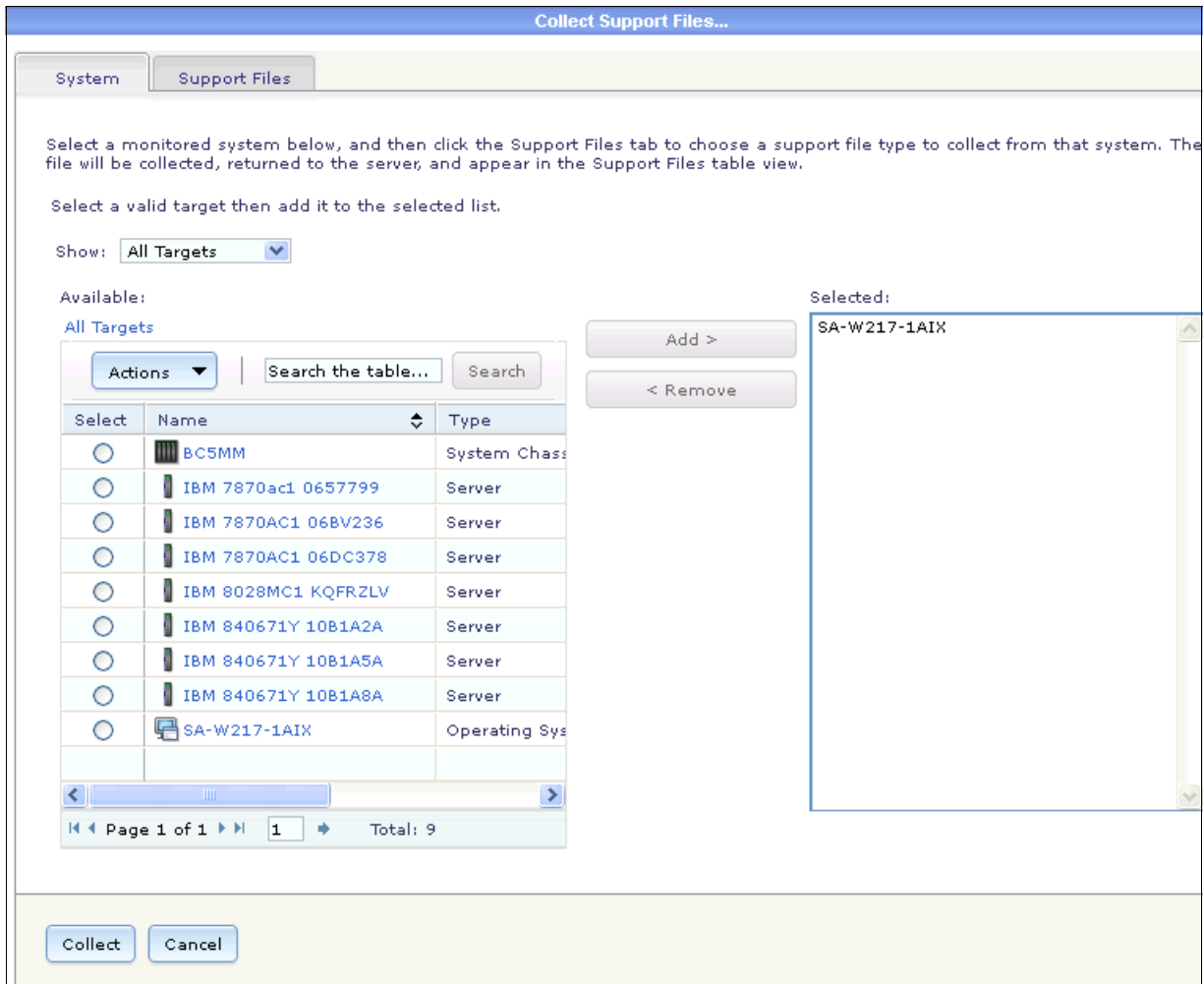


Figure 3-43 Monitored systems

- Click the **Support Files** tab to select the support files (Figure 3-44).

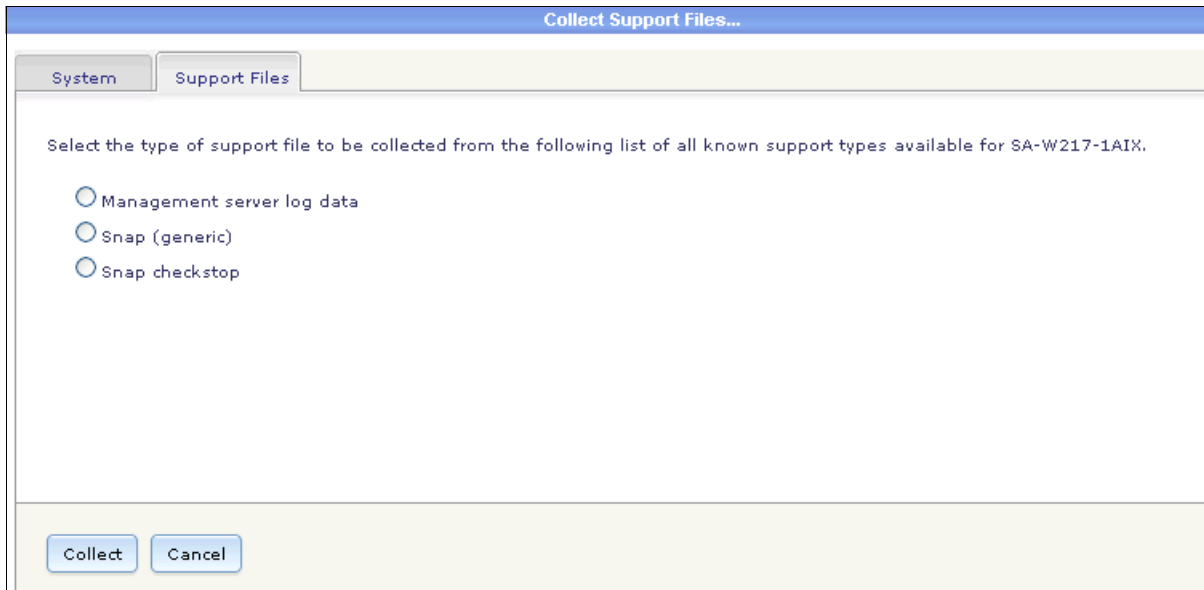


Figure 3-44 Collect Support Files

- Figure 3-44 displays the type of support file to collect. Select the required option and click **Collect**.
- On the window that is shown in Figure 3-45, you can select the support files to send to IBM. After submission, you can delete files manually. However, Service and Support Manager removes support files after seven days after the successful file transmission of data to IBM.

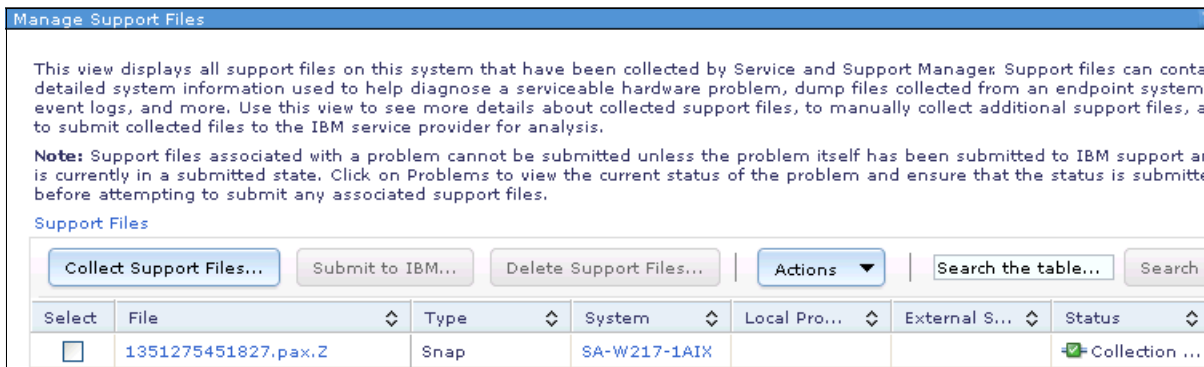


Figure 3-45 Snap files

3.5 Event logs

You can work with the event logs that the Systems Director stores on the server. One predefined Event Action Plan is available with the action Log All Events. This Event Action Plan writes all events of the Systems Director server to a local event log.

3.5.1 Settings

Configure the settings for the event log in the left pane of the Systems Director web interface by clicking **Settings** → **Event Log Preferences** (Figure 3-46).

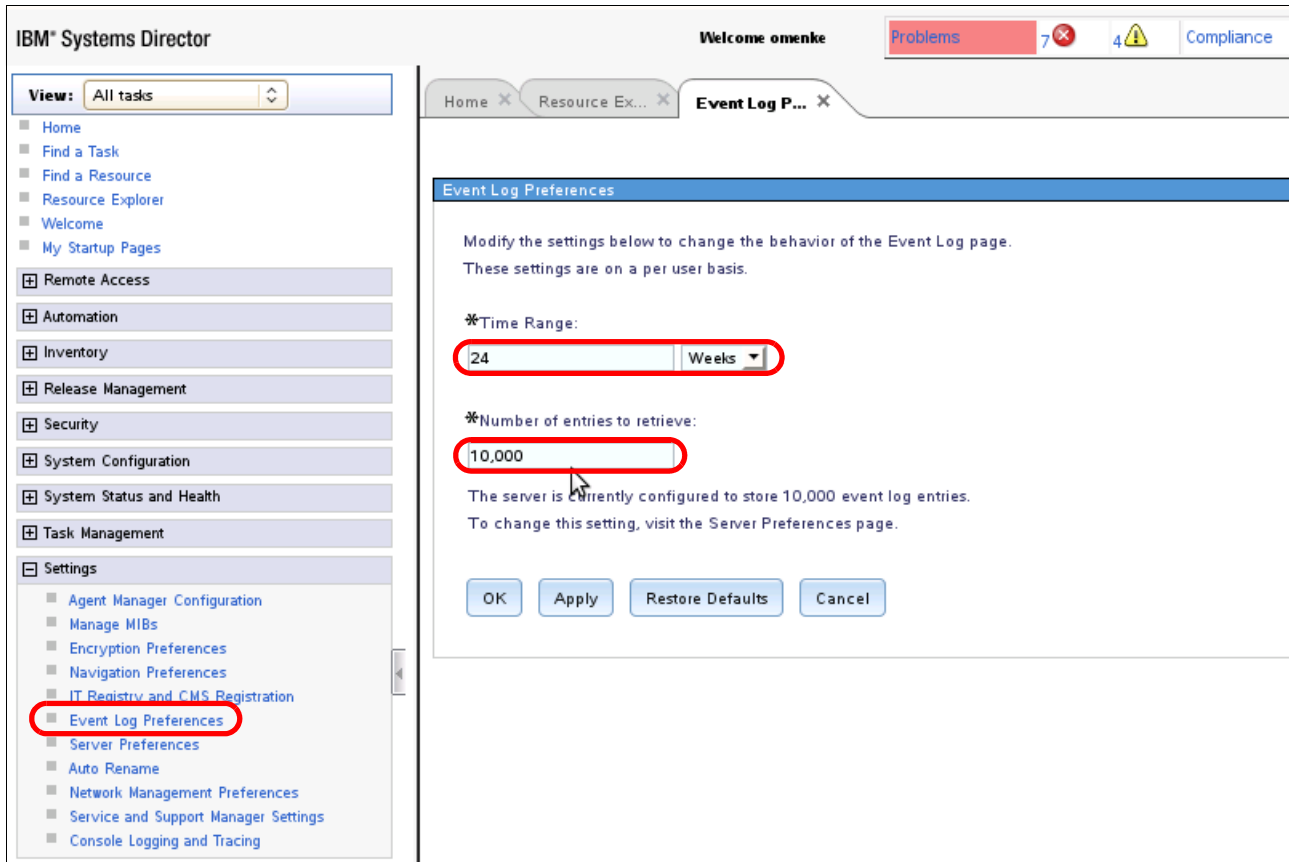


Figure 3-46 Settings for event log preferences

In the Settings window (Figure 3-46), you can select the time range that is reflected in the event log listings. Set a time range for hours, days, or weeks.

You can set the number of event log entries to retrieve. The maximum number for the server is 10,000 entries. If you set more than 10,000 entries, you see an error message (Figure 3-47).

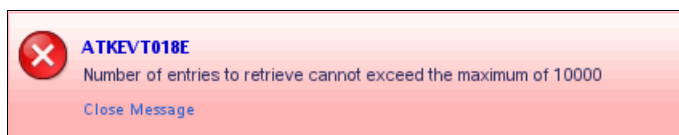


Figure 3-47 Error message when the number of entries exceeds the maximum number of 10,000

The default settings are 24 hours and 500 entries for the event log. You can go back to the default values by clicking **Restore Defaults**.

3.5.2 Launching the event log

You can access the Systems Director event log in a number of ways:

- ▶ From the left pane, click **System Status and Health** → **Event Log** (event log for All Systems).
- ▶ From the Resource Explorer menu, right-click a group (event log for the complete group) or a single system (event log for this system). Click **System Status and Health** → **Event Log** (Figure 3-48).
- ▶ Also, from the Resource Explorer, select the group or system and click **Actions** → **System Status and Health** → **Event Log** to access the event log.

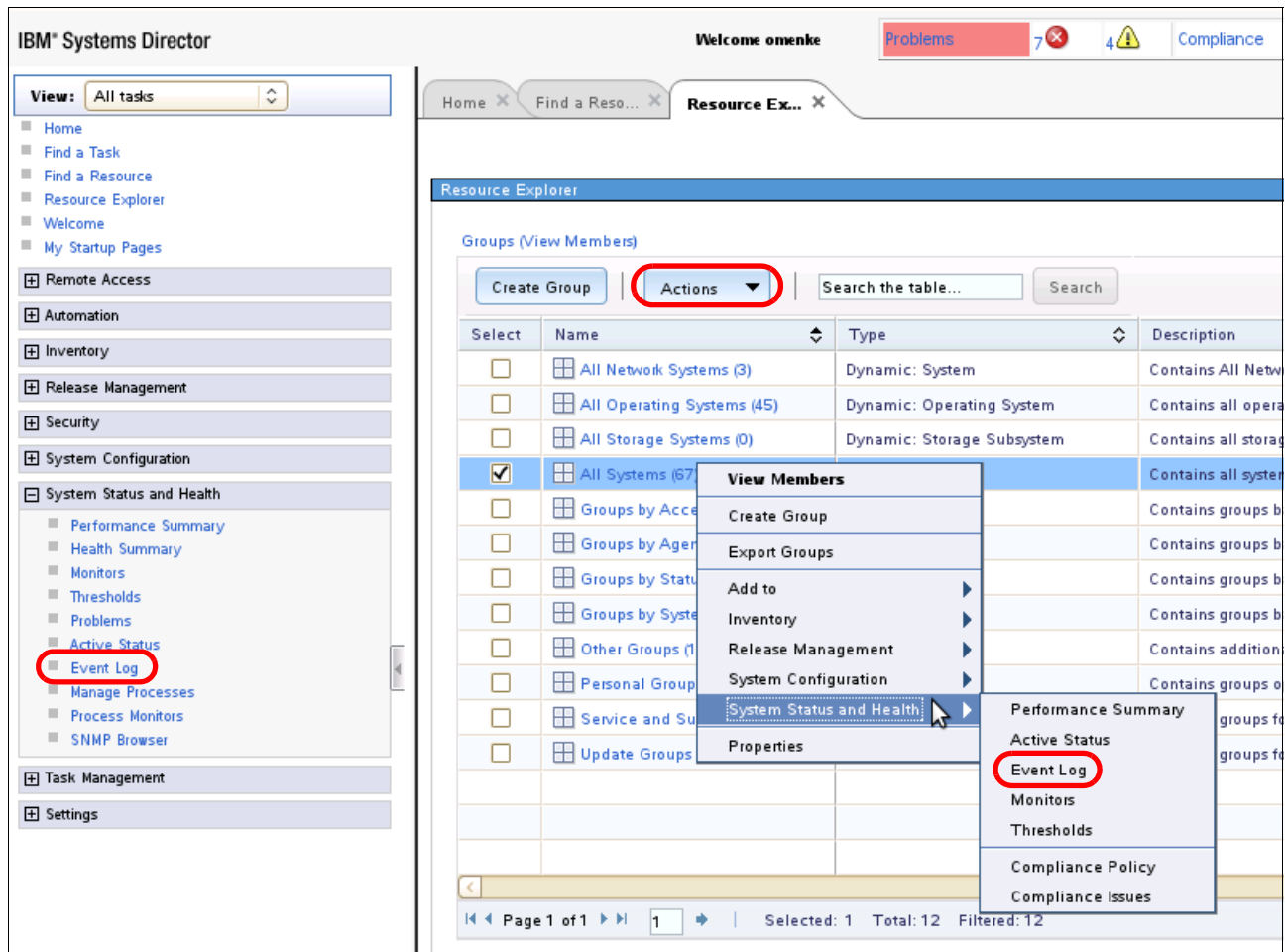


Figure 3-48 Event log access

- ▶ Also, from the Resource Explorer, double-click a single system to see the properties of the system. Select the **Event Log** tab to access the event log for this system as shown in Figure 3-49.

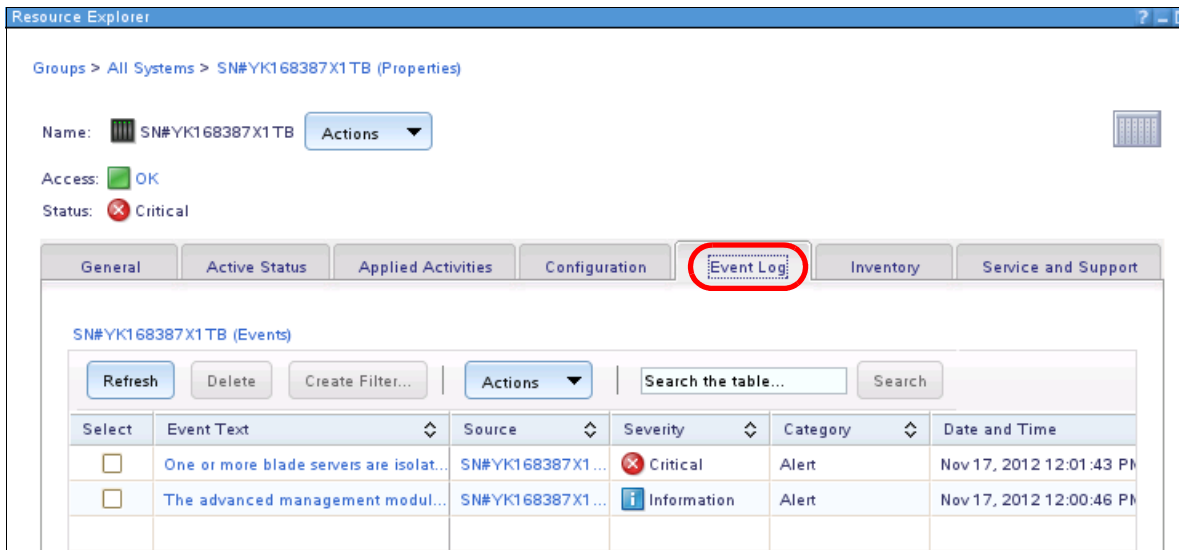


Figure 3-49 Event Log access for a single system

3.5.3 Viewing the event log

When you elect to view the event logs of multiple systems, a new window opens that shows the event log (Figure 3-50 on page 154). All events are listed for the selected time range. Events are listed up to the maximum number that is set for the event log.

The event filter is at the top of the window (Figure 3-50). The use of the event filter is described in 3.5.4, “Using event filters” on page 155. You can sort the events by date and time (default), by severity, or by source and category. Select the column and click the arrow in the top cell of the column. You can also use the search function to find specific events.

Select an event filter to display a specific set of events. Select Event Log Preferences to customize how many events to display.

Event filter:

Last Updated: Nov 17, 2012 5:56:41 PM EST

Events

Select	Event Text	Source	Severity	Category	Date and Time
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 5:31:46 PM
<input type="checkbox"/>	System 9.42.171.86 is online	9.42.171.86	Information	Resolution	Nov 17, 2012 4:23:13 PM
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 3:40:10 PM
<input type="checkbox"/>	System 9.42.171.86 is online	9.42.171.86	Information	Resolution	Nov 17, 2012 12:12:27 PM
<input type="checkbox"/>	One or more blade servers are isolat...	SN#YK168387X1...	Critical	Alert	Nov 17, 2012 12:01:43 PM
<input type="checkbox"/>	The advanced management modul...	SN#YK168387X1...	Information	Alert	Nov 17, 2012 12:00:46 PM
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 10:45:21 AM
<input type="checkbox"/>	System 9.42.171.86 is online	9.42.171.86	Information	Resolution	Nov 17, 2012 10:21:49 AM
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 9:20:20 AM
<input type="checkbox"/>	System 9.42.171.86 is online	9.42.171.86	Information	Resolution	Nov 17, 2012 5:53:22 AM
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 4:59:50 AM
<input type="checkbox"/>	System 9.42.171.86 is online	9.42.171.86	Information	Resolution	Nov 17, 2012 2:07:01 AM
<input type="checkbox"/>	System 9.42.171.86 is offline	9.42.171.86	Information	Alert	Nov 17, 2012 12:42:21 AM

Figure 3-50 Event Log

3.5.4 Using event filters

You can use the event filter to select specific events. With filters, you can easily display only the event log entries that are important to you. With filters, you can easily export log entries for documentation.

The available filters are the same filters that are available in the Event Filter for the event automation plan. Any filters that you create for event automation plans are also visible and usable in this list. Figure 3-51 shows the filter list.

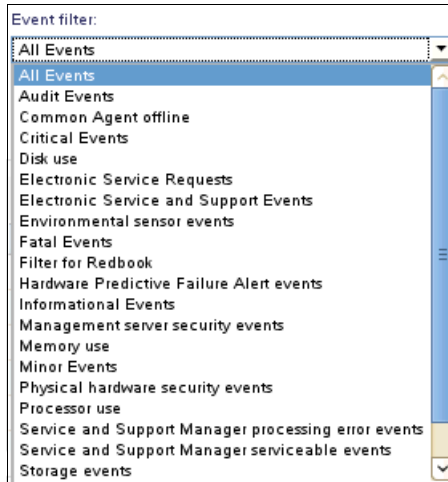


Figure 3-51 Filter list

In our example, we select the critical events as a filter for the event log viewer. The result is shown in Figure 3-52 on page 156. You can see the critical events that are available in the event log of the Systems Director server.

You might see some events with HIST: in front as indicated in Figure 3-52. These events are historical events. Historical events come from system logs from systems that are based on a time range before the actual Systems Director is active.

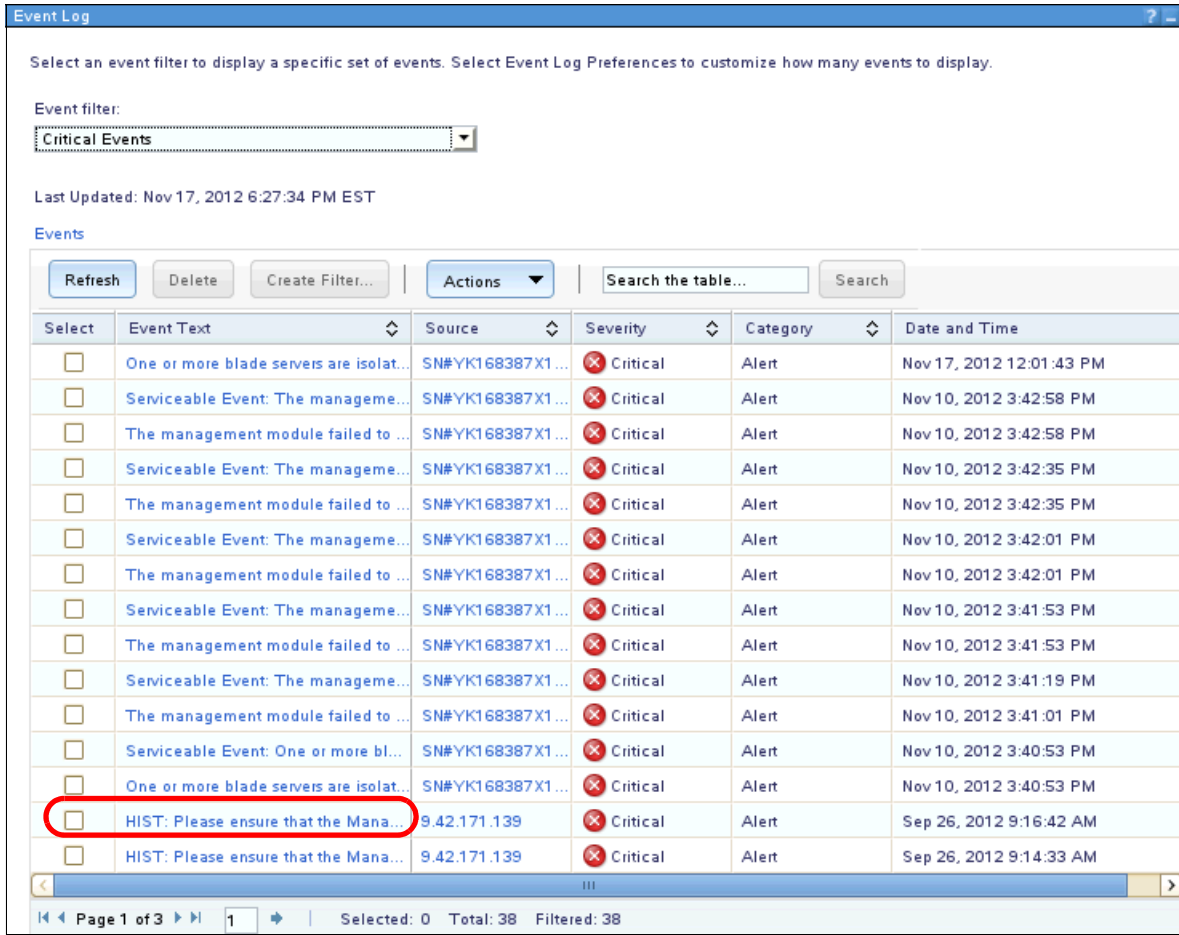


Figure 3-52 Critical event filter is used on the event log

3.5.5 Creating a filter by using an event from the event log

With Systems Director, you can create an event filter that is based on an existing event. This event filter can help you identify all of the events of the same type (for export, as an example).

To create a filter, go to an event and use the following steps:

1. From an existing event, right-click the event and in the pull-down menu, select **Create Filter**. Or, select the event by clicking the adjacent check box and click **Action** → **Create Filter**. See Figure 3-53.

Select	Event Text	Source	Severity	Category	Date and Time
<input type="checkbox"/>	One or more blade servers are isolat...	SN#YK168387X1...	Critical	Alert	Nov 17, 2012 12:01:43 PM
<input type="checkbox"/>	Serviceable Event: The managemen...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:58 PM
<input type="checkbox"/>	The management module failed to ...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:58 PM
<input type="checkbox"/>	Serviceable Event: The managemen...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:35 PM
<input type="checkbox"/>	The management module failed to ...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:35 PM
<input type="checkbox"/>	Serviceable Event: The managemen...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:01 PM
<input type="checkbox"/>	The management module failed to ...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:42:01 PM
<input type="checkbox"/>	Serviceable Event: The managemen...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:41:53 PM
<input type="checkbox"/>	The management module failed to ...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:41:53 PM
<input type="checkbox"/>	Serviceable Event: The managemen...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:41:19 PM
<input type="checkbox"/>	The management module failed to ...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:41:01 PM
<input type="checkbox"/>	Serviceable Event: One or more bl...	SN#YK168387X1...	Critical	Alert	Nov 10, 2012 3:40:53 PM
<input checked="" type="checkbox"/>	One or more blade servers are isolat...		Critical	Alert	Nov 10, 2012 3:40:53 PM
<input type="checkbox"/>	HIST: Please ensure that the Mana...		Critical	Alert	Sep 26, 2012 9:16:42 AM
<input type="checkbox"/>	HIST: Please ensure that the Mana...		Critical	Alert	Sep 26, 2012 9:14:33 AM

Page 1 of 3 | Selected: 1 Total: 38 Filtered: 38

Figure 3-53 Select event to create a filter

2. Enter a name and a short description for the filter (Figure 3-54). Click **OK** to create the event filter that is based on the selected event. The definition for this event is at the bottom of the window.

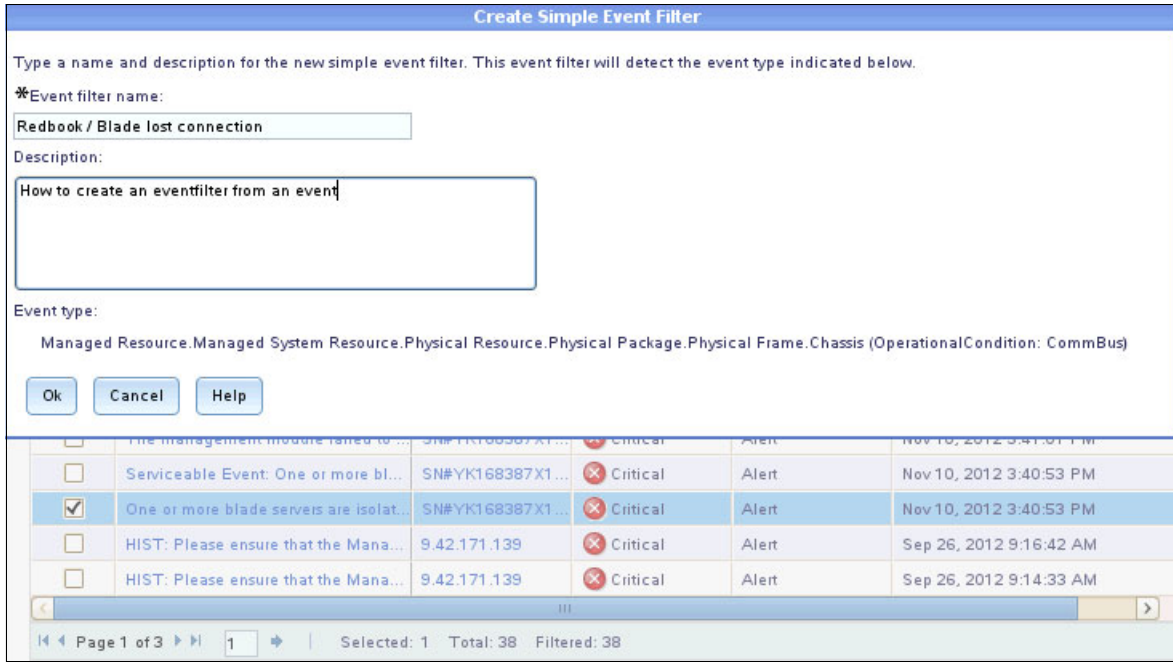


Figure 3-54 Creating a filter from an event

3. A message appears that the event filter is created successfully (Figure 3-55). If there are problems, you see an error message instead. Fix the problem and create the event filter after you fix the problem.

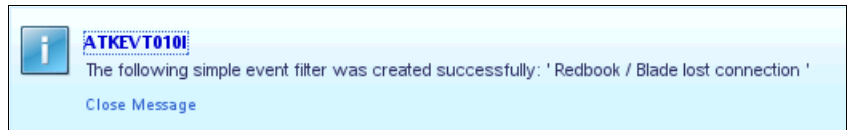


Figure 3-55 Creation of filter successful

3.5.6 Command-line tools

The following command-line commands are available to work with the Systems Director event log:

- smcli evtlog** Set parameter for event log
- smcli lsevtlog** List event log
- smcli rmevtlog** Delete entries or complete event log

Example 3-3 shows the following information:

- ▶ The actual size with the **-s** option. Our example shows 791 entries in the event log.
- ▶ The setting for the maximum value with the **smcli evtlog -m** command.
- ▶ The command to set the maximum to a new value, in our example, 9500 with the **-M 9500** option.

Example 3-3 Example for the smcli evtlog

```
SLES11:/opt/ibm/director/bin #./smcli evtlog -s
791
SLES11:/opt/ibm/director/bin #./smcli evtlog -m
10000
SLES11:/opt/ibm/director/bin #./smcli evtlog -M 9500

SLES11:/opt/ibm/director/bin #./smcli evtlog -m
9500
SLES11:/opt/ibm/director/bin #
```

You can use the **smcli lsevtlog** command to read the event log. The following options are useful:

- e "EventFilter_name"** Show events only for this event filter
- s** Present a summary view of the event
- T** Filter for a time range (value in hours)
- o** Display the unique IDs that are associated with the event-log entries in addition to other information
- t** Filter on a system type, such as operating system

In Example 3-4, we use the **-e "CriticalEvents" -T 192 -o** parameters. These parameters list all critical events in the last 192 hours and the object identifiers (OIDs) for the events. Example 3-4 shows one critical event in the specified time range. The OID for this event (0x2ab) is listed.

Example 3-4 smcli lsevtlog command

```
SLES11:/opt/ibm/director/bin #./smcli lsevtlog -e "Critical Events" -T 192 -o
11/17/12 12:01 PM, One or more blade servers are isolated from the management
bus., SN#YK168387X1TB (0x175b), Managed Resource.Managed System Resource.Physical
Resource.Physical Package.Physical Frame.Chassis (OperationalCondition: CommBus),
Critical-Alert, 0x2ab
SLES11:/opt/ibm/director/bin #
```

Example 3-5 on page 160 shows how to delete an event from the event log with the **smcli rmevtlog** command.

Use this command if many events of the same type are in the log and you want to clean up the log. Or, you generated test log entries that you want to delete from the log.

You can use the **-a** option to delete the complete log or use the **-e %event_oid%** option to delete specific events. In our example, we use the **-e** option to delete the event that is listed in Example 3-4. After we remove the event from the log with the 0x2ab OID, we run the **smcli lsevtlog** command as shown in Example 3-5 on page 160 to list the event. Example 3-5 on page 160 shows that this event does not exist anymore.

Example 3-5 Example for the smcli rmevtlog command

```
SLES11:/opt/ibm/director/bin #./smcli rmevtlog -e 0x2ab
SLES11:/opt/ibm/director/bin #
SLES11:/opt/ibm/director/bin #./smcli lsevtlog -e "Critical Events" -T 192 -o
SLES11:/opt/ibm/director/bin #
```

For detailed information about the commands in our example, see the Systems Director Information Center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_event_log_and_history_cmds.html

3.6 Automation Manager

Use Automation Manager to create and use event automation plans.

The event automation plan consists of two parts:

- ▶ Event filter
- ▶ Event action

You can create and assign the event automation plan, event filter, and event action through the GUI or through the command line.

The following topics are described:

- ▶ 3.6.1, "Creating an event automation plan" on page 161
- ▶ 3.6.2, "Creating an event filter" on page 172
- ▶ 3.6.3, "Creating an event action" on page 182
- ▶ 3.6.4, "Using the CLI for event automation plans" on page 188

3.6.1 Creating an event automation plan

To view and create the event automation plan, go to the Systems Director web interface. Select either **Automation** → **Event Automation Plans** on the left pane or the event automation plan link under the Automation Manager as shown in Figure 3-56.

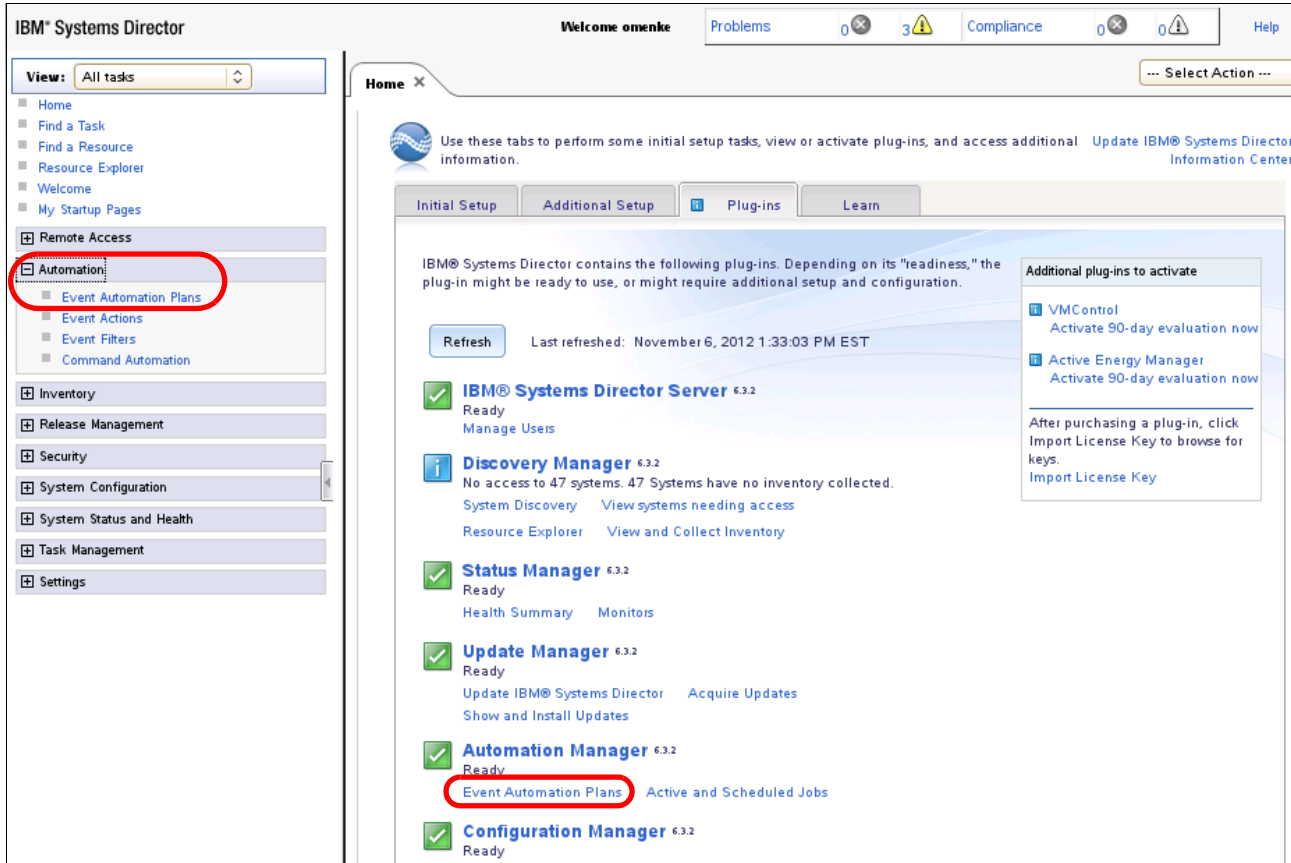


Figure 3-56 Launching Automation Manager

You can see the existing event automation plans, the targets to which they are assigned, the status of the plan, the time range that is defined for the plan, and a description, if available.

You can edit an existing event automation plan, create an event automation plan that is based on an existing event automation plan, or create an event automation plan.

In our example, we create an event automation plan that is named book-EAP:

1. In the Event Automation Plans window, click **Create** (Figure 3-57).

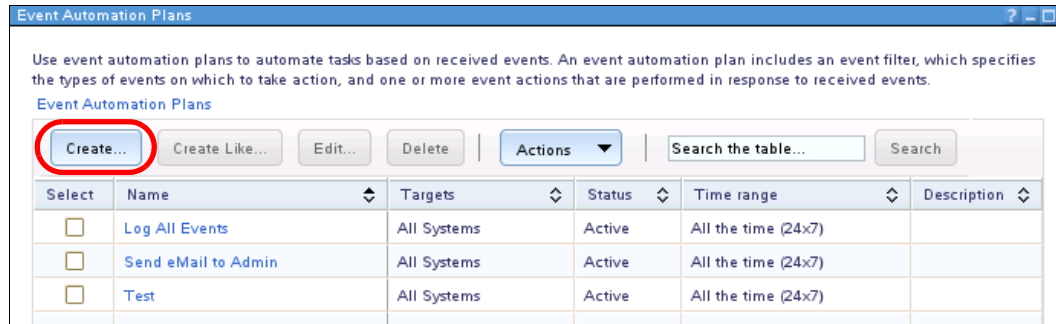


Figure 3-57 Event Automation Plans windows

2. The Create Event Automation Plan wizard opens at the Welcome window (Figure 3-58). Click **Next** to continue.

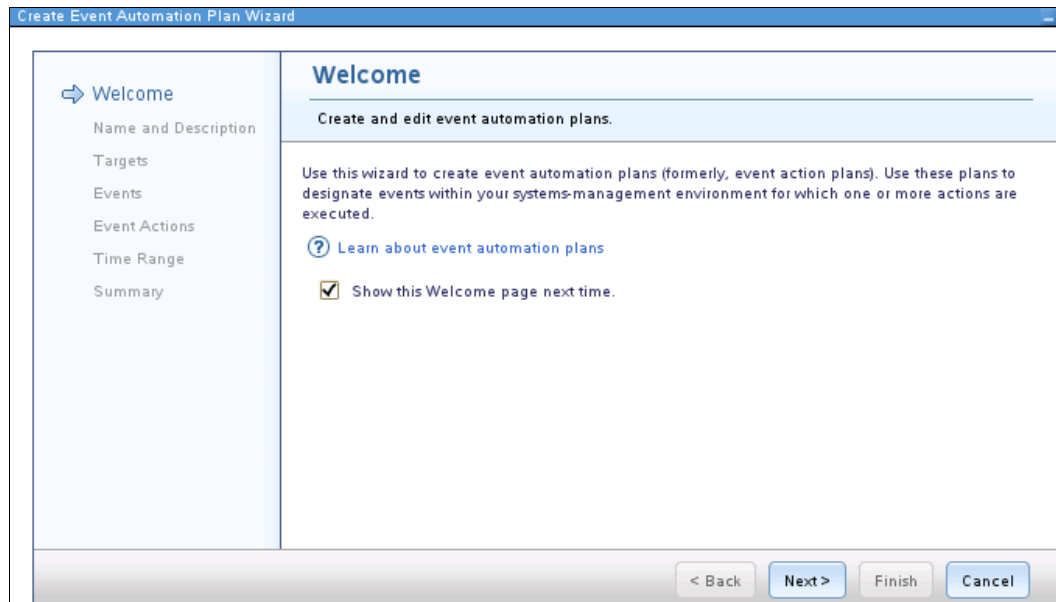


Figure 3-58 Create Event Automation Plan wizard: Welcome panel

3. In the Name and Description step (Figure 3-59), give your event automation plan a name and suitable description. In our example, we name the event automation plan that we created book-EAP. Click **Next** to continue.

The screenshot shows a window titled "Create Event Automation Plan Wizard". On the left is a vertical navigation pane with the following steps: "Welcome" (checked), "Name and Description" (highlighted with a right-pointing arrow), "Targets", "Events", "Event Actions", "Time Range", and "Summary". The main area is titled "Name and Description" and contains the instruction "Type a name and a description for this event automation plan." Below this, there is a field labeled "*Name:" with the text "book-EAP" entered. Underneath is a larger text area labeled "Description:" containing the text "EAP for Demo - how to create an EAP -". At the bottom right of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 3-59 Create Event Automation Plan wizard: Name and Description

- In the next window (Figure 3-60), define the targets for which this event automation plan works. You can select groups or an individual system as the target for this event automation plan.

Selecting groups can be helpful when you have different administrative or management groups. In our example, we select All Systems. To select systems or a group, select the system or group in the left column and then click **Add**. When finished, click **Next**.

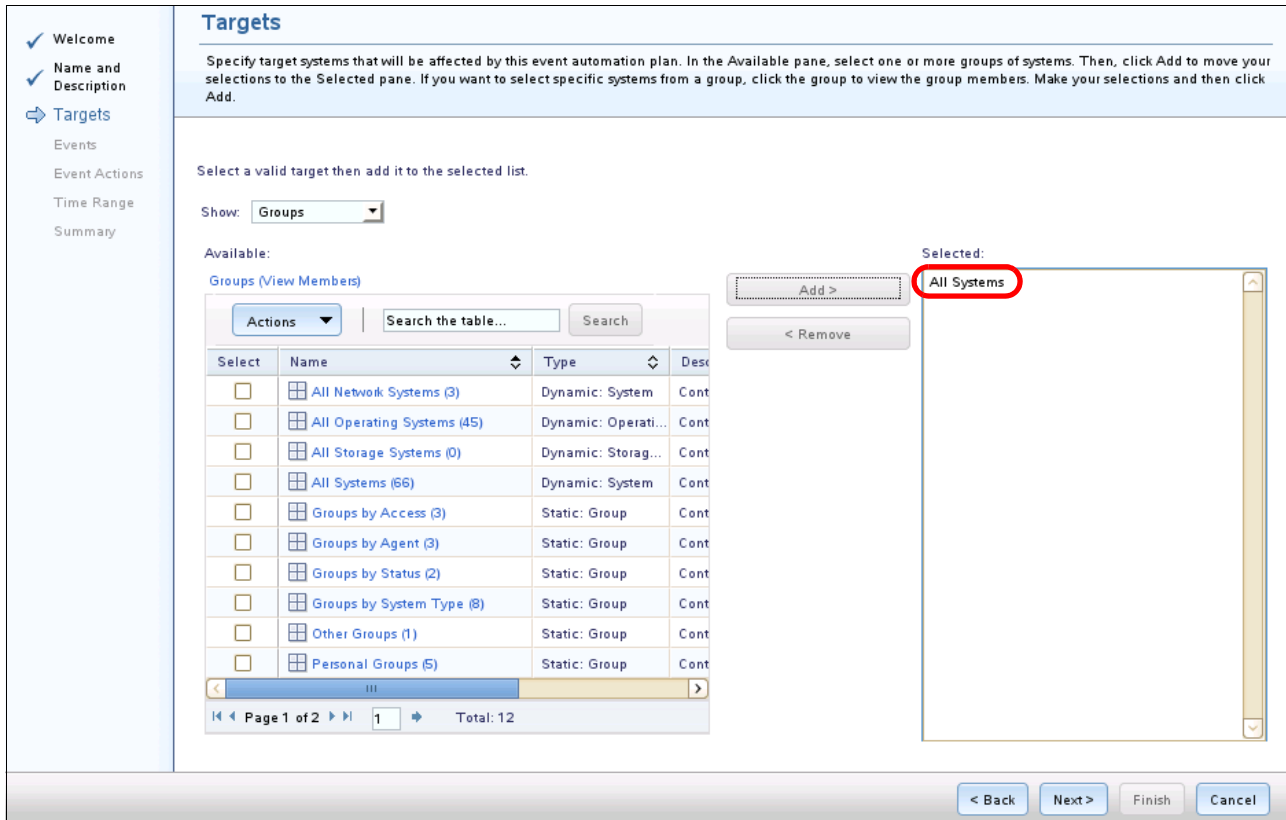


Figure 3-60 Create Event Automation Plan wizard: Target selection

5. In the Events window (Figure 3-61), select the filter for events.

Various filter types are available:

- Common event filters are predefined filters that monitor for common functions, such as hardware events. Examples are fan failures or processor usage (Figure 3-61). The common event filters are predefined and cannot be changed or enhanced. If you need more complex criteria, select the Advanced Event Filters. You can select some of the common event filters to use in an event automation plan.

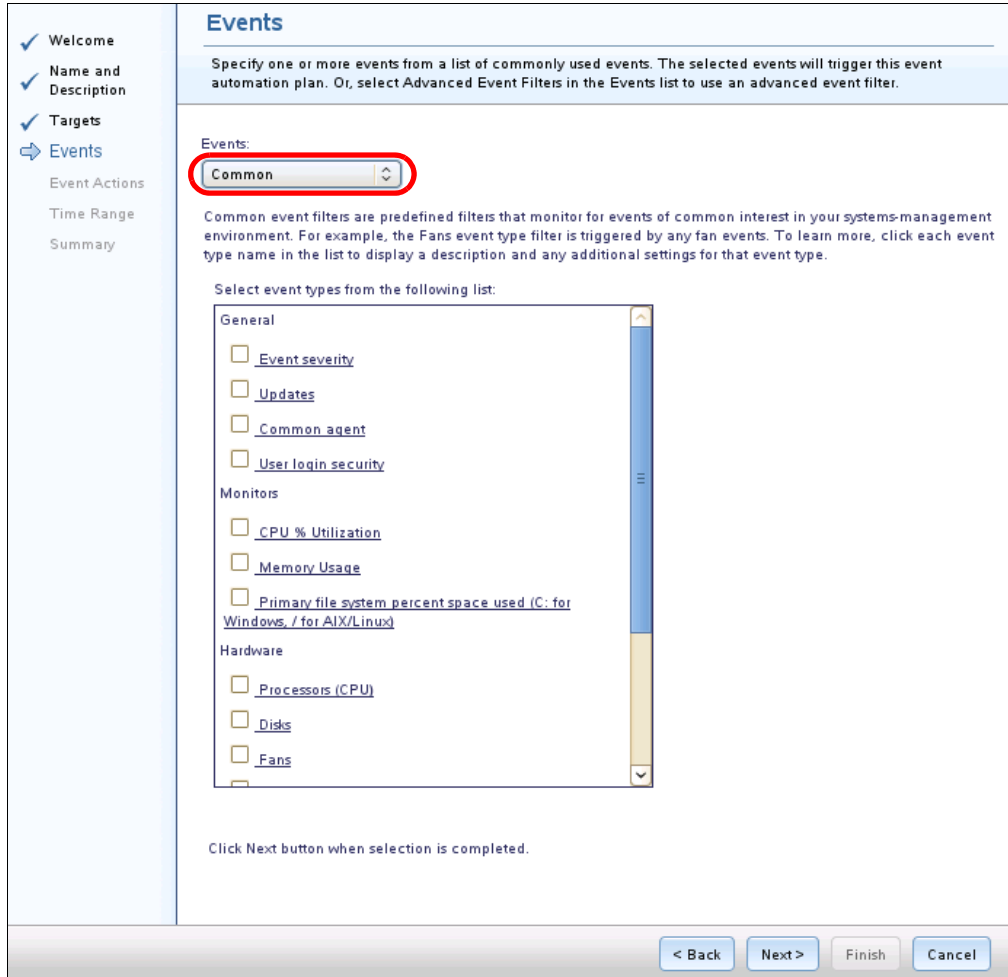


Figure 3-61 Create an event automation plan: Common filter

- Advanced event filters are used for monitoring specific events, single system events, or events that are based on severity (Figure 3-62). Predefined common event filters are available, but you can edit or enhance the advanced event filter. Only one advanced event filter can be selected for an event automation plan.

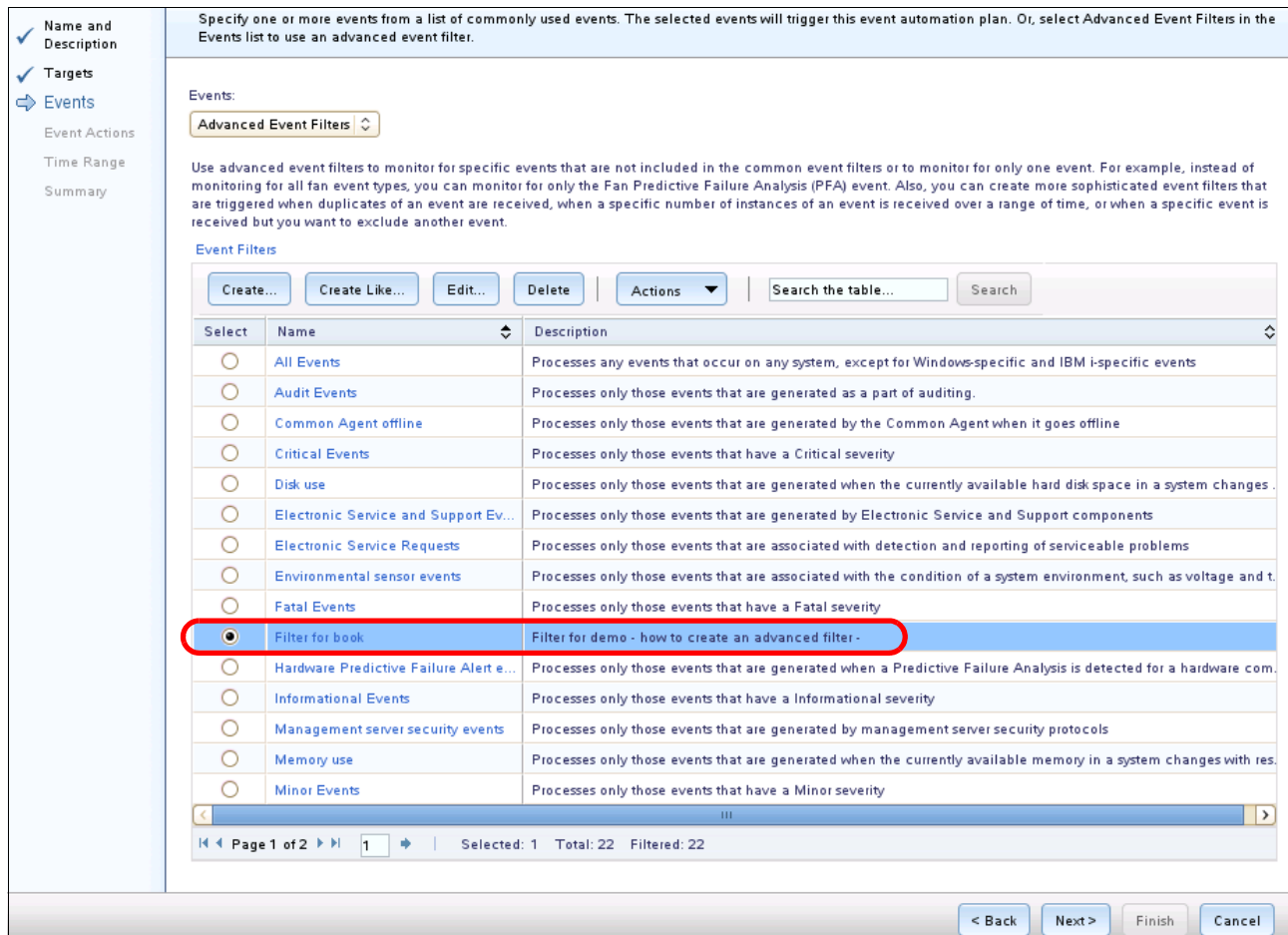


Figure 3-62 Create Event Automation Plan wizard: Advanced event filter

When you select the advanced event filter, you can use predefined filters or create your own. How to create your own filter is described in 3.6.2, “Creating an event filter” on page 172.

In our example, we created the event filter named `Filter for book`. When you select the filter that you want to use, click **Next**.

6. In Figure 3-63, specify the event action for the event automation plan to perform on the target systems when the filter criteria is met. By default, Systems Director comes with only one predefined event action, which is named Add to the event log. Select an existing event action or create an event action. Creating an event action is described in 3.6.3, “Creating an event action” on page 182.

In our example, we use the created event action named Mail to book (Figure 3-63). You can select more than one action for an event automation plan. All of the selected actions run if the event that is monitored and filtered occurs.

After you select the action that you want to use, click **Next**.

The screenshot displays the "Event Actions" configuration window. On the left is a navigation pane with options: Welcome, Name and Description, Targets, Events, Event Actions (selected), Time Range, and Summary. The main area is titled "Event Actions" and contains the instruction "Specify one or more actions that will occur when this event automation plan is triggered." Below this is a toolbar with buttons for "Create...", "Create Like...", "Edit...", "Delete", and an "Actions" dropdown menu. A search bar is also present. The main content is a table with the following data:

Select	Name	Type	History
<input type="checkbox"/>	Add to the event log	Add to the event log	Not saved
<input type="checkbox"/>	eMail	Send an e-mail (Internet SMTP)	Not saved
<input type="checkbox"/>	eMail to Admin	Send an e-mail (Internet SMTP)	Not saved
<input checked="" type="checkbox"/>	Mail to book	Send an e-mail (Internet SMTP)	Not saved

At the bottom of the window, a status bar indicates "Page 1 of 1", "Selected: 1", "Total: 4", and "Filtered: 4". Navigation buttons for "< Back", "Next >", "Finish", and "Cancel" are located at the bottom right.

Figure 3-63 Create Event Automation Plan: Event Actions selection

7. On the next window, specify when the event automation plan can be activated. This time-range constraint can be helpful if you use one event automation plan for work days and another event automation plan for the weekend. You can create the event automation plan that works from Monday to Friday. And, you can create another event automation plan that works from Saturday to Sunday (Figure 3-64).

In our example, we choose All the time (24x7). But if you want, you can change it later by editing the created event automation plan. After you select the time range, click **Next**.

Time Range

(Optional) Specify any time-range constraints for this event automation plan.

All the time (24x7)

Custom

To specify certain days in a time range, select the day from the list and click Add. To specify times during a day, clear the All day check box, set the start and end of the time range, and click Add. You can add more than one time range. The start and end of the time range is rounded to the nearest 15-minute interval. For example, if you specify a time range that starts at 10:10 and ends at 1:35, the event automation plan uses 10:15 and 13:30 for the time range.

Beginning day and time: Sunday 6:00 AM

Ending day and time: Sunday 7:00 AM All day

Add

Specified time range:

Remove

< Back Next > Finish Cancel

Figure 3-64 Create Event Automation Plan wizard: Define a time range

- In the next window (Figure 3-65), you see the summary for the event automation plan that you defined. Specify whether to activate the event automation plan by selecting the check box (default) after you click **Finish**.

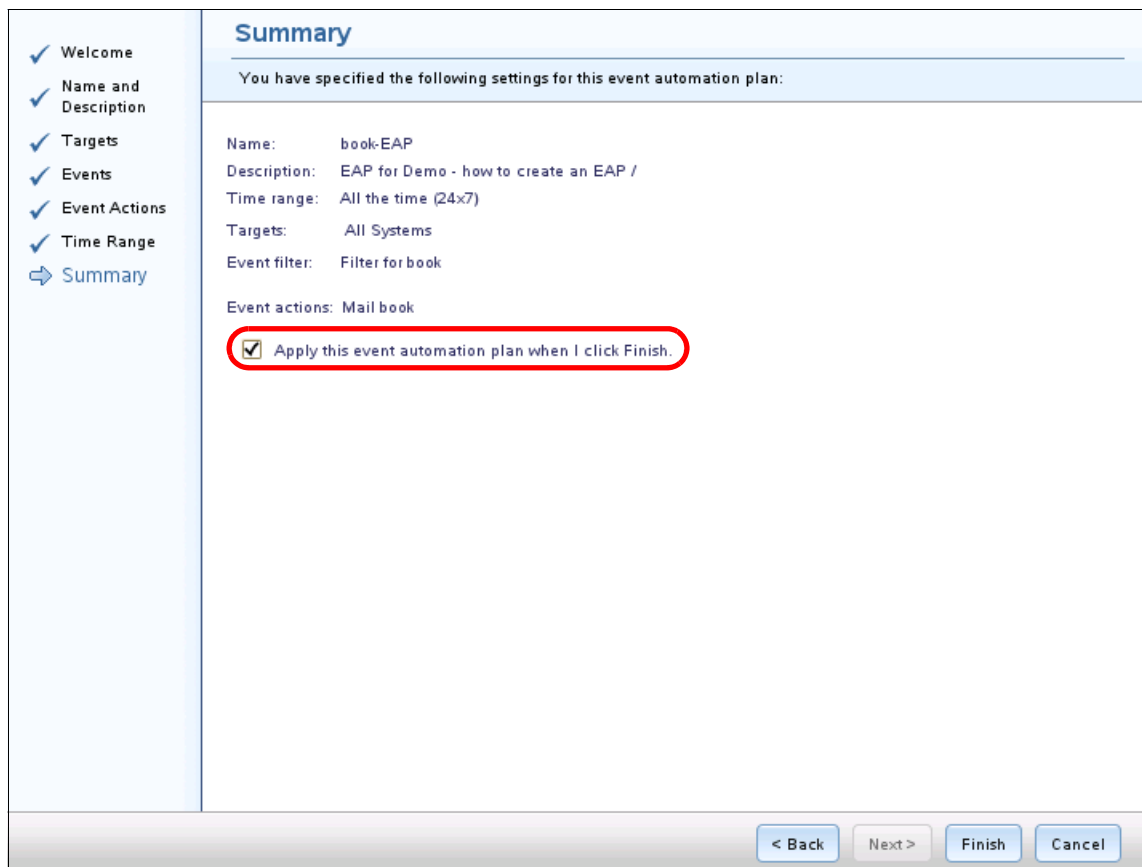


Figure 3-65 Create Event Automation Plan wizard: Summary View

9. Now, you are back on the Event Automation Plans window. You can see the new event automation plan that you created (Figure 3-66).

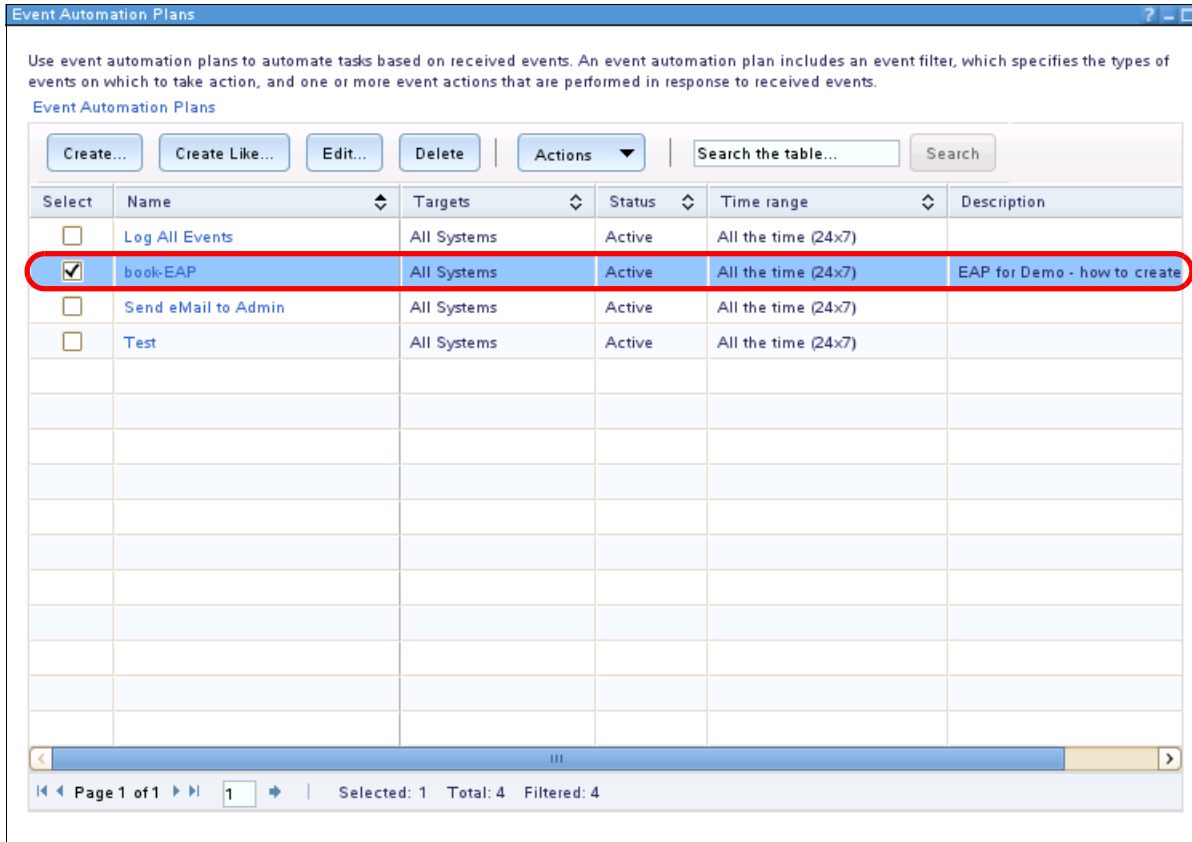


Figure 3-66 Event Automation Plans window

The event automation plan is active and works for the defined systems and time with the defined action.

You can create as many event automation plans as you want, but keep the number of event automation plans to a minimum. If you have too many event automation plans, it can get confusing and you might get multiple alerts for each event.

You can use the GUI to export the event automation plan as a CSV file to use for documentation. On the Event Automation Plans window, select the plans that you want to export by clicking the associated check box. Then, select **Actions** → **Export** as shown in Figure 3-67.

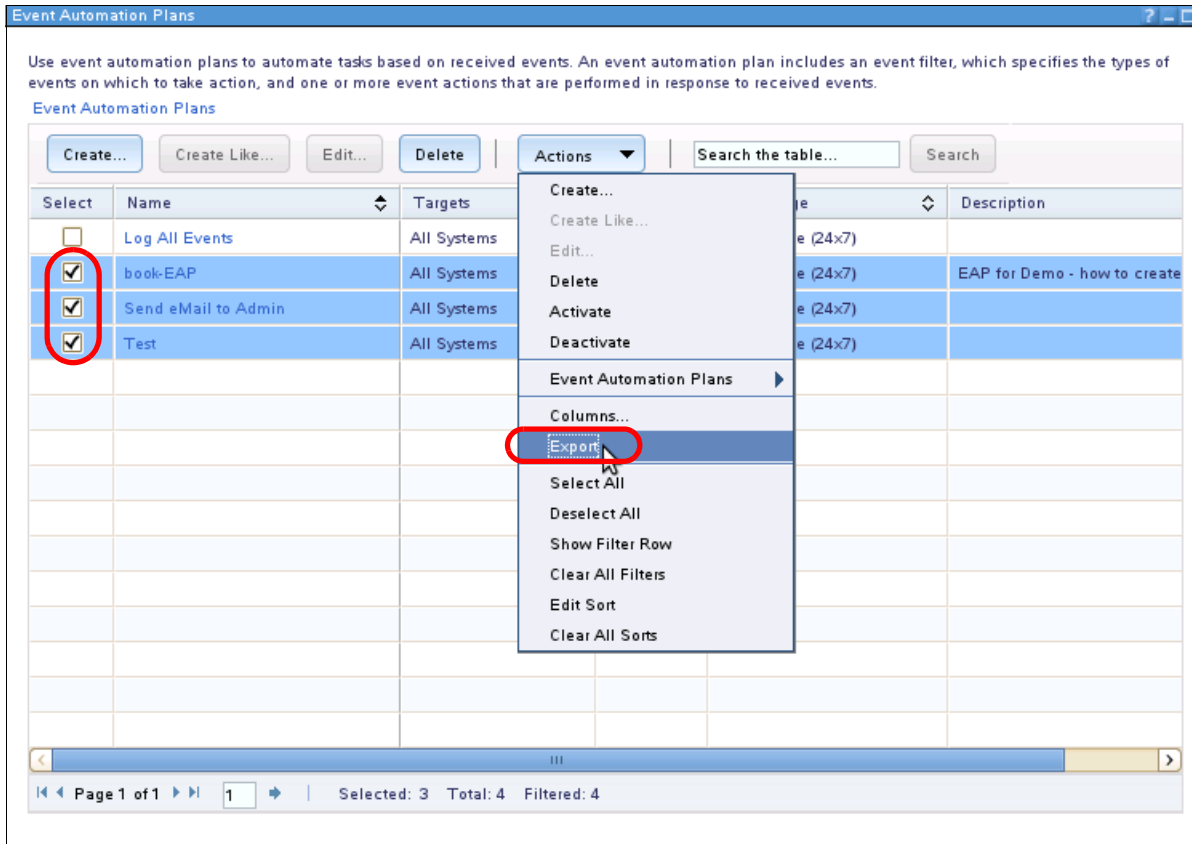


Figure 3-67 Export the event automation plans

A window opens so that you can select the directory where you want to save the event automation plan (Figure 3-68). The name of the file is Event_Automation_Plans.csv.

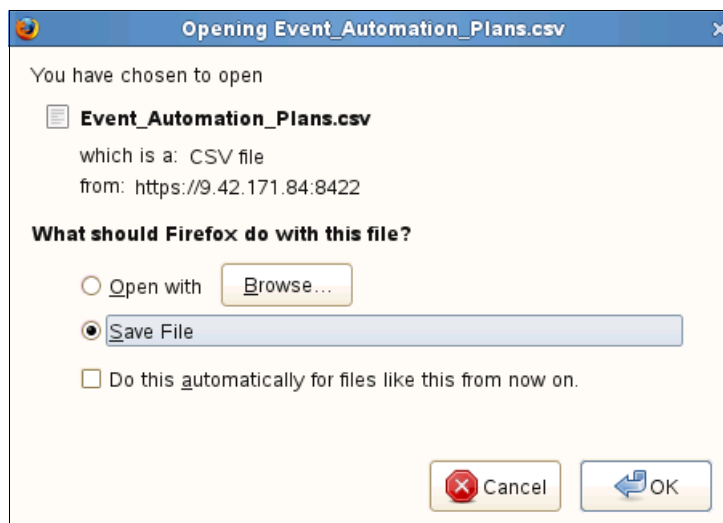


Figure 3-68 Save the Event_Automation_Plans.csv file

If you want to export the event automation plan for use on another system or for backup and recovery, use the `smcli` command line. The use of the `smcli` command line is described in 4.3.1, “Exporting systems and settings” on page 225 and in 4.3.3, “Importing systems and settings” on page 228.

3.6.2 Creating an event filter

You can create an event filter from within the Create Event Automation Plan wizard. Or, select **Automation** → **Event Filters** on the left tab of the Systems Director home page as shown in Figure 3-69.

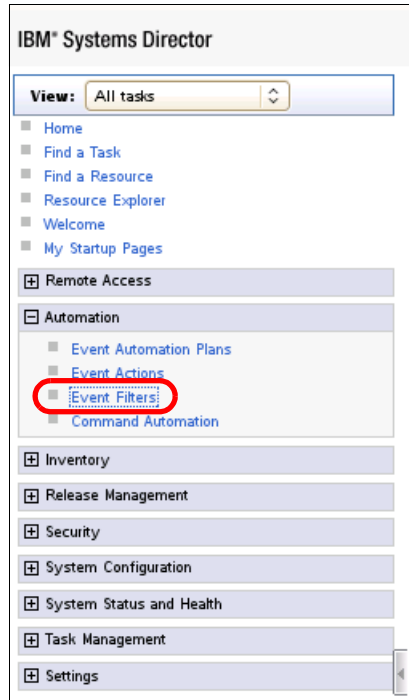


Figure 3-69 Selecting Event Filters

From this link, you are taken to the Event Filters page (Figure 3-70). Figure 3-70 shows the same list of filters in the Create Event Automation Plan wizard (Figure 3-62 on page 166).

Follow these steps to create an event filter:

1. In Figure 3-70, click **Create** to create an event filter.

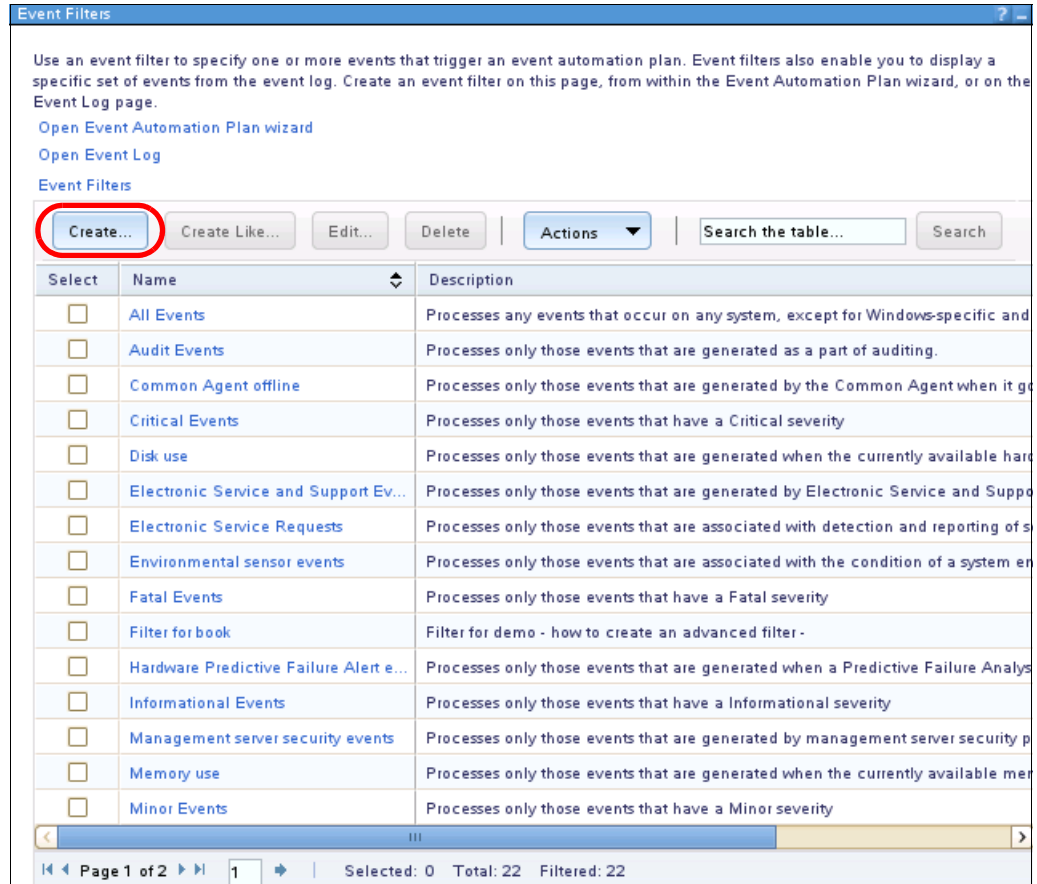


Figure 3-70 Listing of the event filters

2. The Create Event Filter wizard starts and displays the Welcome page (Figure 3-71). Click **Next** to continue.

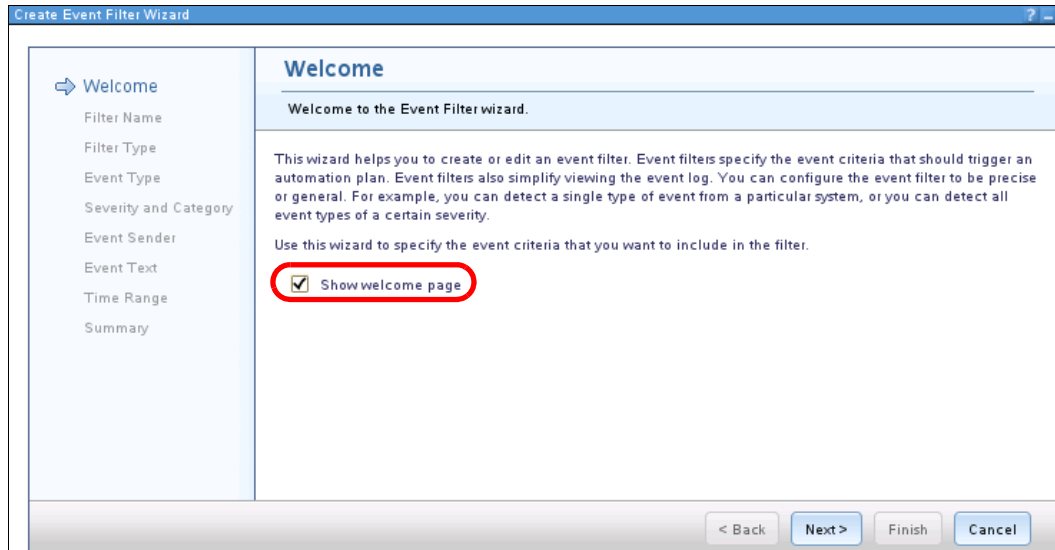


Figure 3-71 Create Event Filter wizard: Welcome window

3. In the Filter Name window (Figure 3-72), enter the name and the description for the filter. In our example, we use the name `Filter for book`. You can also add a short description for the filter. Click **Next** to continue.

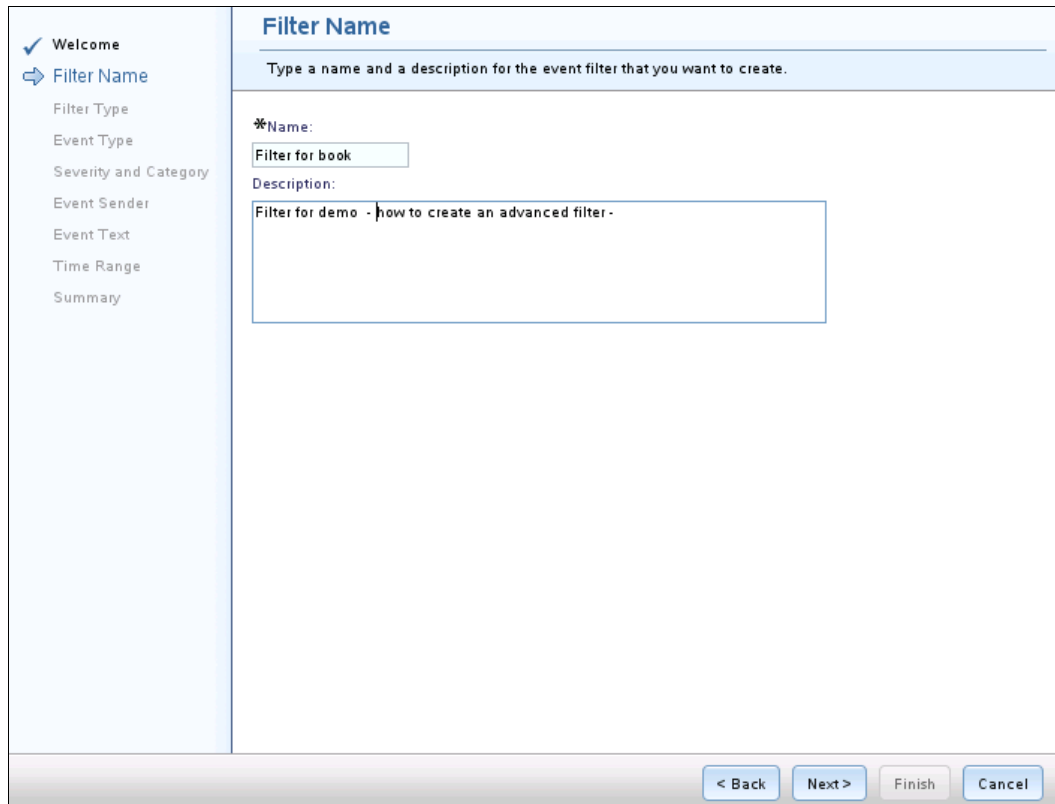


Figure 3-72 Create Event Filter wizard: Filter Name

4. In the Filter Type window (Figure 3-73), select the type of filter that you want to create. We select the simple event filter for our example.

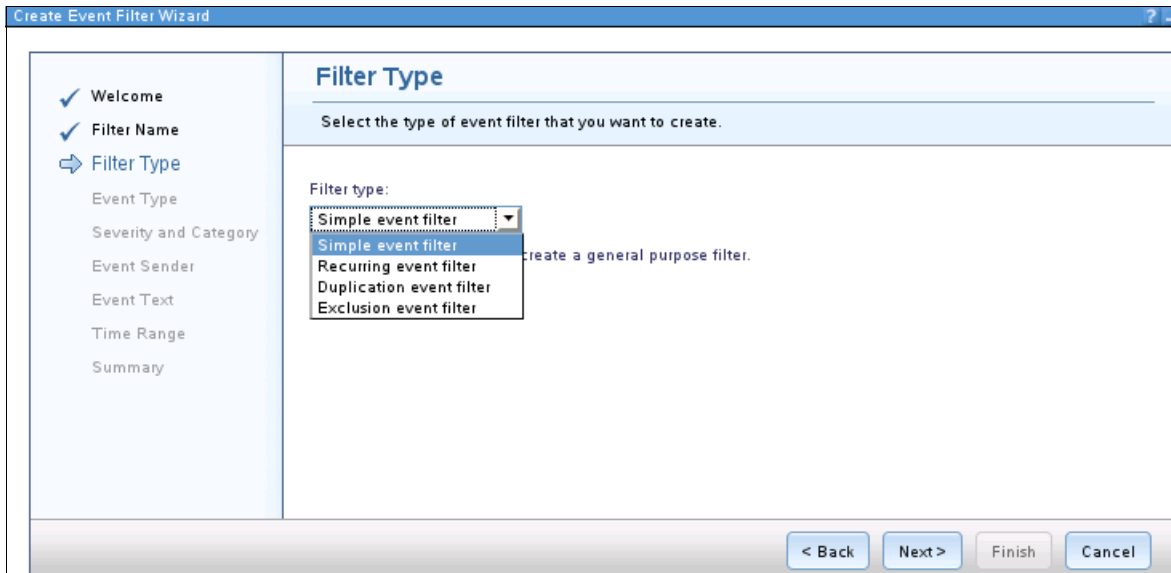


Figure 3-73 Create Event Filter wizard: Filter Type

The following types of filters are available. Select the filter type and click **Next**.

- Simple event filter: Use the general-purpose filter to create your own filter.
- Recurring event filter: Use this filter to trigger only when the included event meets the filter criteria more than one time in the defined time range.
- Duplication event filter: Use this filter to ignore duplicate events.
- Exclusion event filter: Use this filter to exclude a specific event type from a larger list of event types that you included in the event.

5. In the Event Type window, Figure 3-74, select the filter type and define the filter type that you want use. The following event types are available:

- Default: Include all events except IBM System i® message queue events, which can be selected by clicking the check box, and Windows specific events. If you need to select the Windows specific events, use the Custom type.
- Common: Include events that are often used in the custom environment. The custom environment events include general events, such as information about updates or user security events. General events also include hardware events, such as power, storage, fan, or processor events. You can add the system message events.
- Custom: Include events of certain category, type, or value. The available events depend on the system types, operating systems, or protocols that you use in your Systems Director environment.

In our example, we use the default events. In our example, we use Default filter type, which includes all events. Click **Next** to continue.

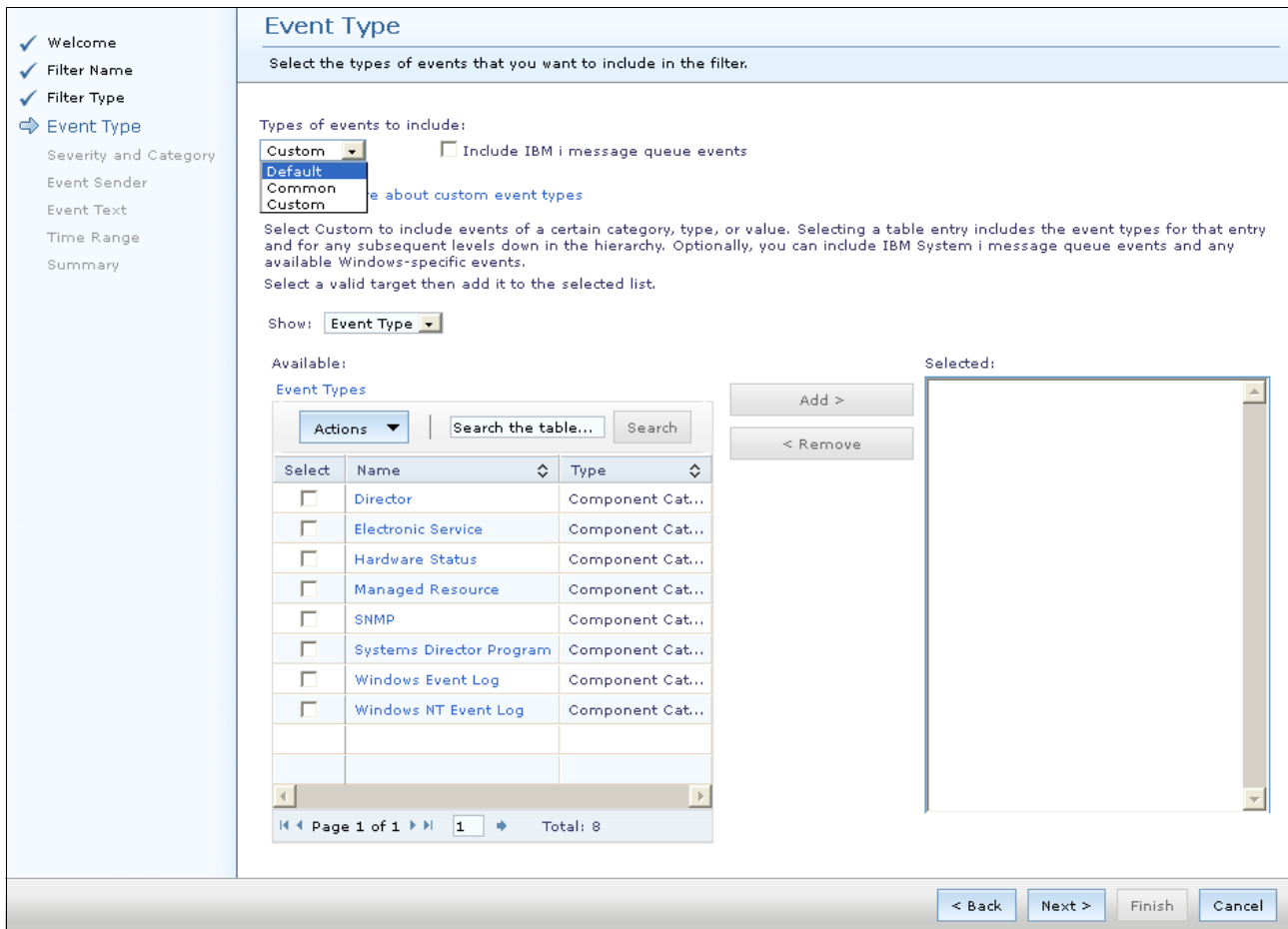


Figure 3-74 Create Event Filter wizard: Event Type selection

6. In the Severity and Category window (Figure 3-75), select the severity and category for the filter. Various severities are available for events in Systems Director:

- Fatal
- Critical
- Minor
- Warning
- Informational
- Unknown

Two event categories are available:

- Alert
- Resolution

In our example, we use the Fatal, Critical, and Warning severities and the Alert category as shown in Figure 3-75. Click **Next** to continue.

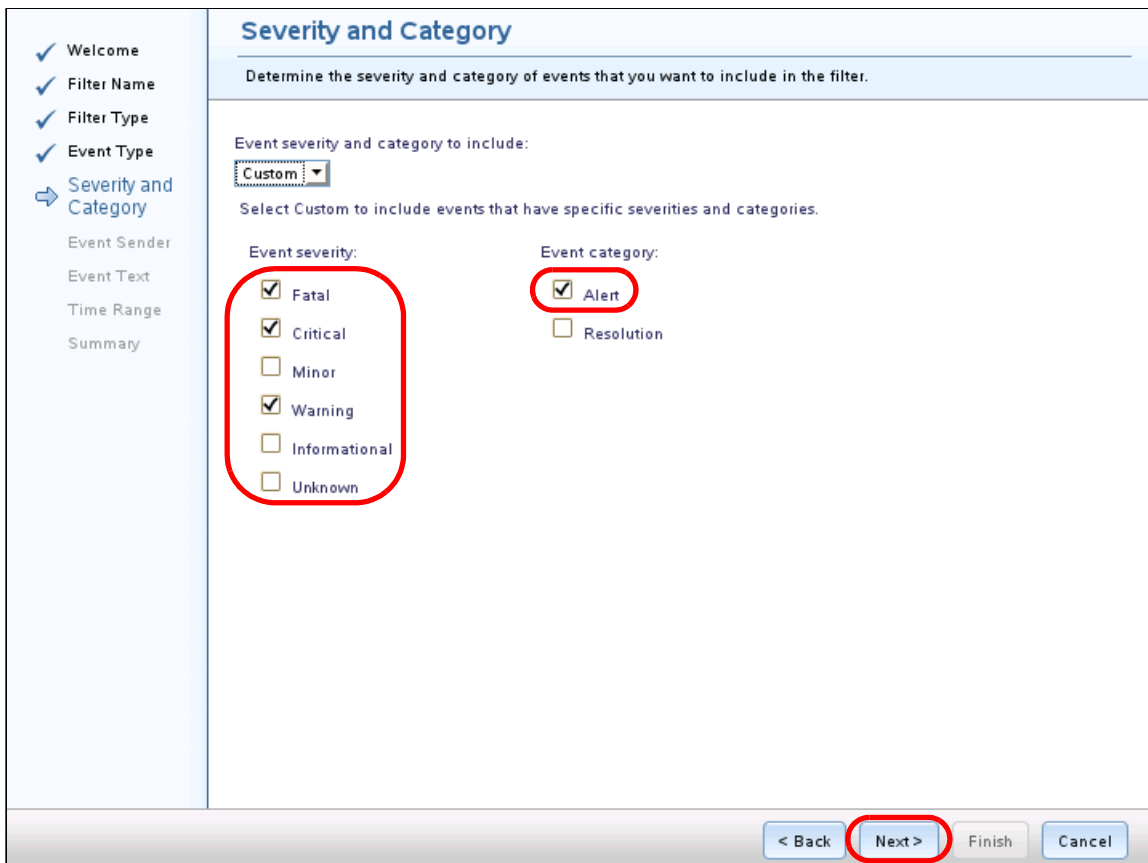


Figure 3-75 Create Event Filter wizard: Severity and Category selection

7. In the Event Sender window (Figure 3-76), select the system that you want to include in this filter:
 - Default: Includes all systems that Systems Director discovered or can access.
 - Custom: Select individual systems or groups to include in this filter.

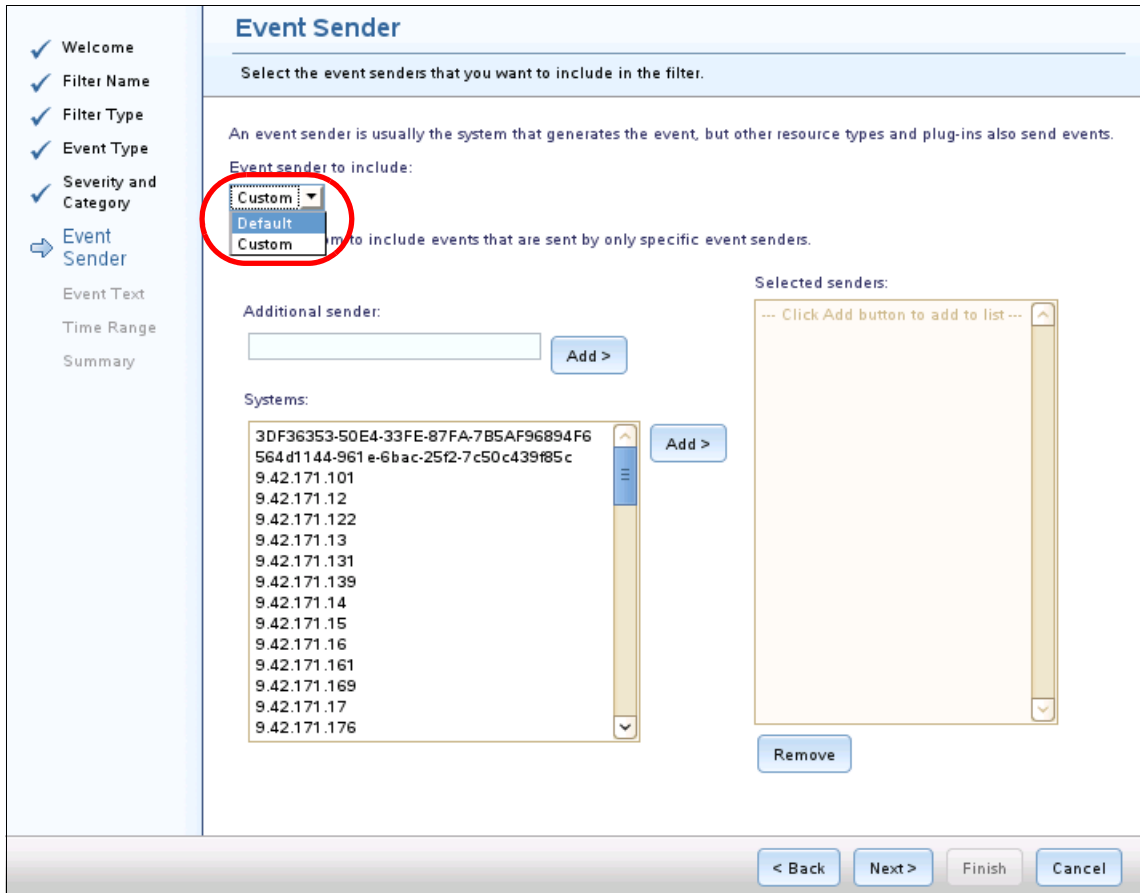


Figure 3-76 Create Event Filter wizard: Event Sender selection

If you select Custom, the window expands (see Figure 3-76). On the left, you see a box to enter additional systems and a list of systems. Select the systems and click **Add** to add these systems to the Selected senders list. The filter works for only these systems.

In our example, we use Default to select all systems because we use the filter in the event automation plan. In the event automation plan, you can also select the systems for which the event automation plan works. If you select specific systems on this window and different systems in the event automation plan, no events are handled through the event automation plan. So, if you plan to use the filter in an event automation plan, leave the selection on Figure 3-76 as Default. Use Custom when you want to use the filter for event capture only. Do not use Custom in an event automation plan with event actions that use it.

Click **Next** to continue.

8. In the Event Text window (Figure 3-77), select the event text. Two selections are possible:
- Default: Include all event text.
 - Custom: Filter for specific event text. This option might be interesting if you want only specific events from systems. Select Custom to specify a word, separate words, or a phrase that you want to include in the filter. The filter is triggered by only those events that you include in the filter that also contain the specified text.

In our example, we leave the selection on Default. Therefore, we want to get all alerts from the alert type that we chose earlier. Click **Next** to continue.

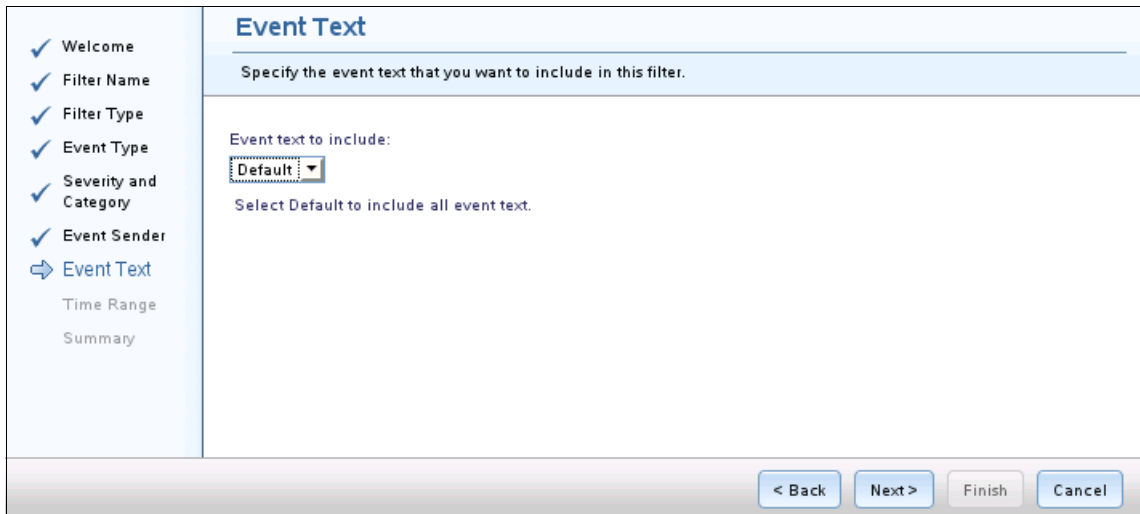


Figure 3-77 Create Event Filter wizard: Event Text selection

9. In the Time Range window (Figure 3-78), select a time range for the filter. You can either select All (the default), which is 24x7, or Custom. If you select Custom, you can define the days or hours that the filter works.

In our example, we use the filter that is in the event automation plan; therefore, we keep the All setting on Figure 3-78. We also can set a time range in the Event Automation Plan wizard. We do not want a conflict between the settings in the filter and the settings in the event automation plan. The setting in Figure 3-78 is used if you use a filter only to capture events and not with an action.

Click **Next** to continue.

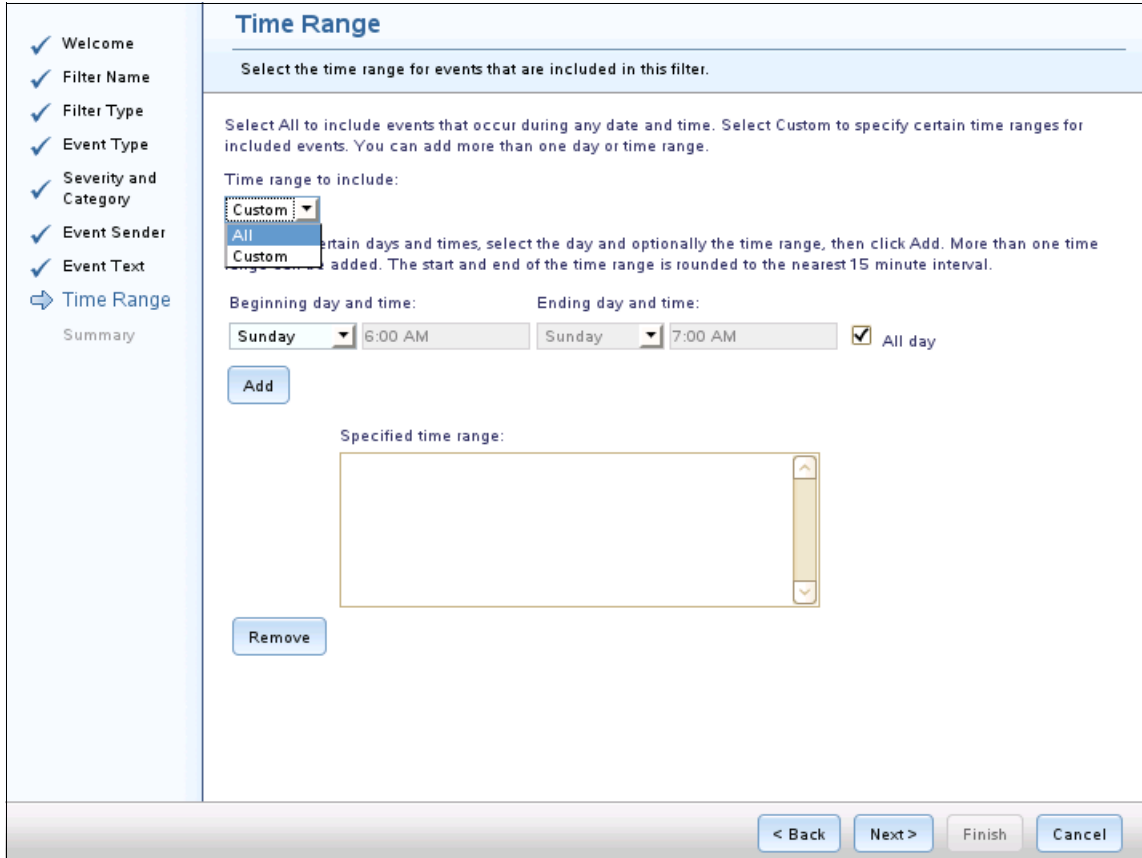


Figure 3-78 Create Event Filter wizard: Time Range selection

10. The last window of the wizard shows the summary view for the filter that you defined (Figure 3-79). Check the settings and information and click **Finish** to create this filter.

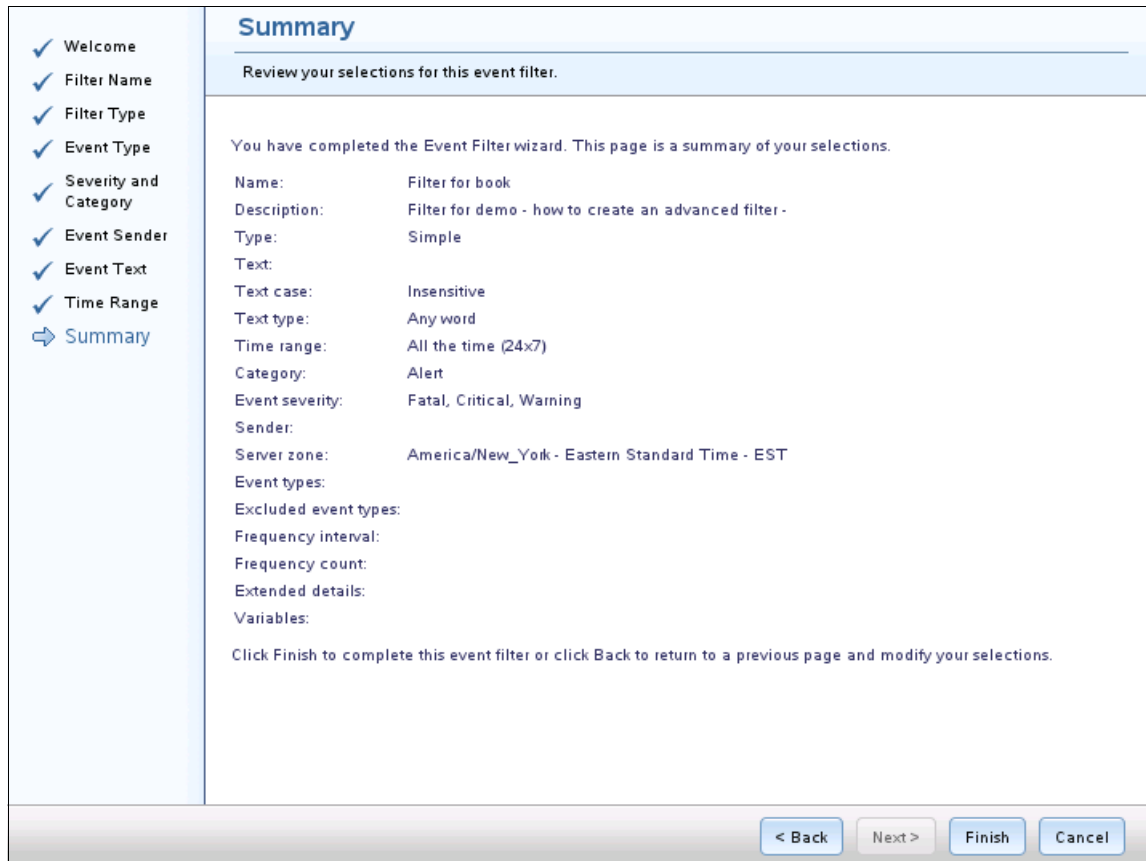


Figure 3-79 Create Event Filter wizard: Summary view

The filter is created. The filter is available in the list of the filters and can be used in event automation plans.

3.6.3 Creating an event action

You can create event actions in the Create Event Automation Plan wizard or select the Event Actions link on the left panel of the Systems Director home page (Figure 3-80).

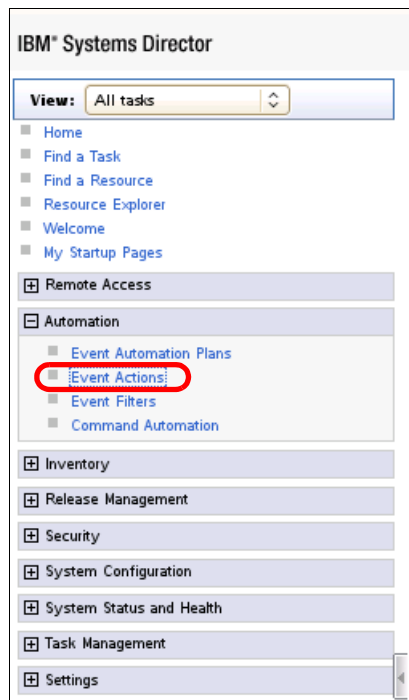


Figure 3-80 Selecting Event Actions

From this link, you are taken to the Event Actions page (Figure 3-81). This list shows the same actions in the Create Event Automation Plans wizard (Figure 3-63 on page 167).

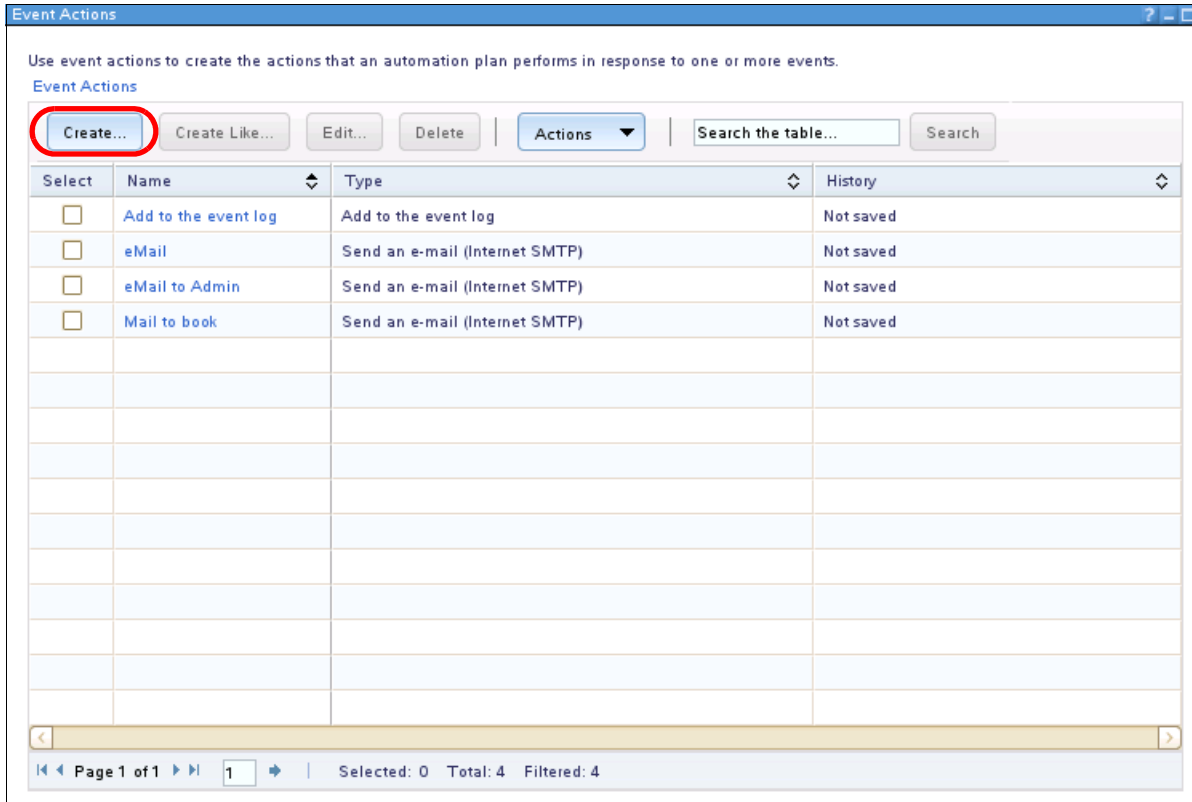


Figure 3-81 Event Actions

Follow these steps to create an event action:

1. Click **Create** in Figure 3-81 to create an event action. Or, select an existing action and click Edit to change an existing action.

2. Figure 3-82 opens with the available event actions.

Create Action

Select the type of action that you want to create.

▾ |

Select	Name	Type
<input type="radio"/>	Send an e-mail to a mobile phone	Common
<input type="radio"/>	Start a program on a system	Common
<input type="radio"/>	Start a program on the management server	Common
<input type="radio"/>	Send an e-mail (Internet SMTP)	Common
<input type="radio"/>	Start a program on the system that generated the event	Common
<input type="radio"/>	Static group: add or remove the event-generating system	Advanced
<input type="radio"/>	Post to a newsgroup (NNTP)	Advanced
<input type="radio"/>	Send an SNMP inform request to an IP host	Advanced
<input type="radio"/>	Start a task on a system that generated the event	Advanced
<input type="radio"/>	Timed alarm that generates an event	Advanced
<input type="radio"/>	Modify an event and send it	Advanced
<input type="radio"/>	Set an event system variable	Advanced
<input type="radio"/>	Send events to Syslog server	Advanced
<input type="radio"/>	Send an SNMP trap reliably to a NetView host	Advanced
<input type="radio"/>	Log to a log file	Advanced

Figure 3-82 Create Action (Page 1 of 2)

Page 2 of the list of available actions is shown in Figure 3-83.

Create Action

Select the type of action that you want to create.

Actions ▾ | Search

Select	Name		Type
<input type="radio"/>	Send an event to Tivoli Event Integration Facility (EIF) probe	◇	Advanced
<input type="radio"/>	Static group: add or remove group members		Advanced
<input type="radio"/>	Timed alarm that starts a program		Advanced
<input type="radio"/>	Send an SNMP trap to an IP host		Advanced
<input type="radio"/>	Start a task on a specified system		Advanced
<input type="radio"/>	Send a Tivoli Enterprise Console event		Advanced

Page 2 of 2 | 2 | Selected: 0 Total: 21 Filtered: 21

OK Cancel Help

Figure 3-83 Create Action (Page 2 of 2)

3. Select an action and click **OK**. In our example, we choose “Send an e-mail (Internet SMTP)” as shown in Figure 3-84.

The screenshot shows a 'Create Action' dialog box with a table of actions. The 'Send an e-mail (Internet SMTP)' action is selected, indicated by a radio button and a blue highlight. The table has columns for 'Select', 'Name', and 'Type'. Below the table is a pagination bar showing 'Page 1 of 2' and 'Selected: 1 Total: 21 Filtered: 21'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Select	Name	Type
<input type="radio"/>	Send an e-mail to a mobile phone	Common
<input type="radio"/>	Start a program on a system	Common
<input type="radio"/>	Start a program on the management server	Common
<input checked="" type="radio"/>	Send an e-mail (Internet SMTP)	Common
<input type="radio"/>	Start a program on the system that generated the event	Common
<input type="radio"/>	Static group: add or remove the event-generating system	Advanced
<input type="radio"/>	Post to a newsgroup (NNTP)	Advanced
<input type="radio"/>	Send an SNMP inform request to an IP host	Advanced
<input type="radio"/>	Start a task on a system that generated the event	Advanced
<input type="radio"/>	Timed alarm that generates an event	Advanced
<input type="radio"/>	Modify an event and send it	Advanced
<input type="radio"/>	Set an event system variable	Advanced
<input type="radio"/>	Send events to Syslog server	Advanced
<input type="radio"/>	Send an SNMP trap reliably to a NetView host	Advanced
<input type="radio"/>	Log to a log file	Advanced

Figure 3-84 Select an action to configure

4. The configuration window opens for your selected action. The content of the window varies depending on the action that you select. Our example shows the settings for the “Send an e-mail (Internet SMTP)” action (Figure 3-85).

The screenshot shows a configuration window titled "Create Action" for an "E-mail" action. The fields are as follows:

- *Action name: Mail to book
- Description: Mail for demo purpose
- *Send-to e-mail address: admin@itso.ral.ibm.com
- *Reply-to e-mail address: ISD@itso.ral.ibm.com
- *E-mail (SMTP) server (for example, smtp.mycompany.com): smtp.itso.ral.ibm.com
- *E-mail (SMTP) port: 25
- Subject of message: &date &system
- Body of message: &date &time message from &system message: &text

Below the message body, there is a section for inserting event variables:

- Event variable: Date the event occurred (&date)
- Target text field: Body of message:
- Language: English
- Time zone: EST - Eastern Standard Time - EST

Buttons at the bottom include "Test", "OK", "Cancel", and "Help".

Figure 3-85 Configuration window for the Send an e-mail (internet SMTP) action

Set the following information for this example:

- ▶ Type a name for the action. In our example, we type Mail to book.
- ▶ Optional: Type a description for the action. We enter Mail for demo purpose.
- ▶ Enter the send-to email address. We enter admin@itso.ral.ibm.com.
- ▶ You must enter a Reply-to email address. This email address is listed as the sender of the email. This email address must be in the correct format but the email address does not need to exist. For example, you can use noreply@example.com. We use ISD@itso.ral.ibm.com.
- ▶ Enter the Simple Mail Transfer Protocol (SMTP) server that is used in your environment. We use smtp.itso.ral.ibm.com.

- ▶ Enter the port that is used by the SMTP server. The standard port for SMTP is port 25.
- ▶ The next entry is for the subject of the message. The default subject line is `&date &system`, which prints the actual date and the system name that sent the event. You can add additional variables or write your own text. The complete list of variables is at this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.automation.helps.doc%2Ffqm0_c_ea_event_data_substitution_variables.html

As an alternative to typing the variables, the window also includes two list boxes, Event variable and Target text field. Click **Insert** to insert the variable for you.

- ▶ Type the body of the message. The default is `&text` (the event text). In our example, we use a combination of text and variables:

```
&date &time message from &system
message: &text
```

- ▶ The last two fields specify the language and the time zone. Our example uses English and EST- Eastern Standard Time- EST.

Test the event action to confirm that the settings are valid. You can view the resulting email by clicking **Test**. The email that we received from our test is shown in Figure 3-86.

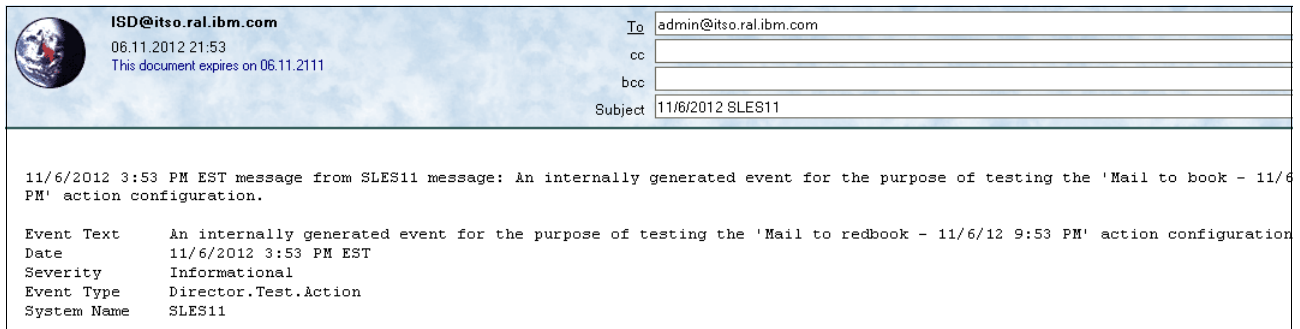


Figure 3-86 Test email from event action

After you confirm that the event action works correctly, click **OK** to save the changes. The action is then shown in the list of available actions.

3.6.4 Using the CLI for event automation plans

There are several available `smcli` commands that you can use to work with event automation plans (Table 3-4).

Table 3-4 Command-line tools for event automation

Command	Purpose
For event automation plans	
<code>lsevtautopln</code>	List information about an event automation plan.
<code>mkevtautopln</code>	Create an event automation plan.
<code>rmevtautopln</code>	Delete one or more event automation plans.
<code>evtautopl</code>	Apply one or more event automation plans to a system or a group. Use this command to remove systems or groups from an event automation plan or activate or deactivate an event automation plan.
<code>chevtautopln</code>	Change an existing event automation plan.

Command	Purpose
For event filters	
lsevtfltr	Display information about an event filter or list all available event filters.
lsevttype	List the event types.
mkevtfltr	Import event filters.
rmevtfltr	Remove event filter.
For event actions	
lsevtact	Display information about available event actions or export event actions to an XML file.
mkevtact	Import event actions.
mkevtactemail	Create a customized event action that sends email over an SMTP server.
mkevtactstpgm	Create a customized action that starts a program.
mkevtacttask	Create a customized action that starts a non-interactive task.
rmevtact	Remove a customized event action.
testevtact	Test a customized event action.

For detailed information about these commands and the options for these commands, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_automation_cmds.html

Example 3-6 creates the “e-mail for test” event action. Example 3-7 on page 190 creates the “Email for Critical Events” event automation plan that is used for critical events.

First, we list the available event action on our Systems Director server with the **smcli lsevtact** command. Then, we create an email event action with the **smcli mkevtactemail** command.

Example 3-6 Create Action Send email

```
SLES11:/opt/ibm/director/bin#./smcli lsevtact
Add to the event log
Mail to book
eMail
eMail to admin
SLES11:/opt/ibm/director/bin#./smcli mkevtactemail -I -p 25 -s "&date &system" -m
"&date &time message form &system : &text "email for test" admin@itso.ral.ibm.com
ISD@ITSO.ral.ibm.com smtp.itso.ral.ibm.com
SLES11:/opt/ibm/director/bin#./smcli testevtact "email for test"
DNZEAP1073I: <informational> The test or the event action was successfully started
SLES11:/opt/ibm/director/bin#
SLES11:/opt/ibm/director/bin#./smcli lsevtact
Add to event log
Mail to book
eMail
eMail to admin
email for test
```

```
SLES11:/opt/ibm/director/bin#
```

We create our “email for critical events” event automation plan by using the **smcli evtautopln** command. First, we list the available event automation plans. Then, we create an event automation plan by using the “Critical Events” filter. Then, we create the “email for test” event action. We assign the new EAP to the “All Systems” group. After these steps, we list the event automation plans that are available now. You can see that the newly created event automation plan is in the list (Example 3-7).

Example 3-7 Create the event automation plan named “email for critical events”

```
SLES11:/opt/ibm/director/bin#
SLES11:/opt/ibm/director/bin#./smcli lsevtautopln
Log All Events
book-EAP
Send eMail to Admin
Test
SLES11:/opt/ibm/director/bin#
SLES11:/opt/ibm/director/bin# ./smcli mkevtautopln -D "Test" -e "Critical Events"
-x "email for test" -N "All Systems" "email for critical events"
SLES11:/opt/ibm/director/bin#
SLES11:/opt/ibm/director/bin#./smcli lsevtautopln
Log All Events
book-EAP
Send eMail to Admin
Test
email for critical events
SLES11:/opt/ibm/director/bin#
```

If you want to see the details or status for an event automation plan, use the **smcli lsevtautopln -l “%EAP-Name%”** command. Example 3-8 lists the detailed information for our newly created “email for critical events” event automation plan.

Example 3-8 List details for the “email for critical events” event automation plan

```
SLES11:/opt/ibm/director/bin# ./smcli lsevtautopln -l “email for critical events”
Name: email for critical events
Description: Test
Status: Active
Event Filter: CriticalEvents
Time Ranges:
    All the time (24x7)
Actions:
    email for test
Targets:
    Group Name: All Systems
SLES11:/opt/ibm/director/bin#
```

3.7 Security

Systems Director security is controlled by two interdependent processes: authentication and authorization.

Authentication is used to determine who can access the Systems Director server. *Authorization* determines the resources to which the user has access. Systems Director uses role-based access control (RBAC) where the administrator assigns roles and permissions to an authenticated user. On that basis, the user can work on resources that are based on the RBAC to which the user is assigned.

The security features of Systems Director enable an administrator to perform the following functions:

- ▶ Manage auditing
- ▶ View and manage authorized users and groups
- ▶ Assign roles and resources to users
- ▶ Manage user properties
- ▶ Create and modify roles
- ▶ Manage permissions that are grouped within a role
- ▶ Use roles to control access to a system
- ▶ Request access to a system
- ▶ Manage credentials and their associated mappings

The following flow allows a user to access or manage a system:

1. User must be authenticated.
2. User must be authorized to perform a task on the selected resource.

3.7.1 Users and groups for authentication

In Systems Director, users and user groups are based on users and groups that are defined in the configured registry. The registry is associated with either the operating system, directory services, such as Lightweight Directory Access Protocol (LDAP), or the domain controller. Systems Director uses the user and group information for authentication and authorization.

Access to particular resources or tasks is governed by restrictions. The restrictions are based on the user ID or user group membership and the roles that are defined for each user. For a user to access the Systems Director server, one of the following conditions must exist:

- ▶ The user is a member of a user group that is authorized for the Systems Director server.
- ▶ The user has administrator privileges on the Windows management server or Windows domain.
- ▶ The user is a root user on the AIX or Linux management server.

In a default Systems Director server installation scenario that uses the local operating system registry, four Systems Director user groups are automatically created. The user groups are created at the operating system level on the management server. Table 3-5 on page 191 lists the user groups, which are used for different access permissions to the Systems Director server.

Table 3-5 Default groups

Default groups	Role	Description
smadmin	SMAAdministrator	Administrator group. Users in this group have administrative access to Systems Director and can perform all administrative tasks. These members can define the available privileges for the smmgr, smmon, smuser, and groupread groups. The privileges that are available to members of the smadmin group cannot be restricted.

Default groups	Role	Description
smmgr	SManager	Manager group. The supported operations are a subset of the SMAdministrator group. The members of this group have all rights except the rights to create or change user permissions and authorizations.
smmon	SMonitor	Monitor group. This group supports some administrative functions, such as monitoring. The members of this group are restricted to read-only functionality.
smuser	SMUser	User group. Members of this group have, by default, no rights and no access to any system or functions.

Members of the root and Administrators group are authorized for all operations on all resources.

The only role that is automatically assigned is to the administrator user ID that installed Systems Director. So, initially, no other user is associated with a role.

If you want to use LDAP or another directory service that the user registry supports, you might need to manually create all the user groups and assign users to them.

The users for Systems Director must be added to one of the groups to get access to the Systems Director GUI.

Authenticating a local user

Systems Director can authenticate user login requests to the registry for the configured operating system. Systems Director uses the local operating system user registry by default.

Follow these steps to create a local operating system user account:

1. Create a user account in the user registry that is associated with the management server. The way that you create the user account depends on the operating system that you use.
2. Add the user as a member of one of the user groups that are defined for Systems Director at the user registry level. You can either use one of the predefined groups or create your own groups. If you create a custom group on the Systems Director server, you must authorize it. (Log in as a member of the smadmin group and then go to **Security** → **Users** → **Authorize Groups**. Or, use the `smcli authusergp` command).
3. Log in to Systems Director web interface as a member of the smadmin group and navigate to **Security** → **Users**. The users that you configured in the previous steps are displayed in the list.

After users are authenticated to Systems Director, you can configure the authorizations for each user to Systems Director tasks and resources.

Authenticating a domain user

Systems Director can authenticate a user from an Active Directory domain to access the Systems Director GUI. Use the following steps to generate the access for the domain user:

1. Create a user account in the Active Directory user registry. For instructions about creating a user account in the domain server user registry, see the Active Directory documentation.
2. Add the Active Directory user to a defined Active Directory global security group. You must create your own Active Directory group if a suitable group does not exist.

3. Add the global group to an authorized local group of the Systems Director server, such as smadmin, smmgr, smmon, or smuser.

Systems Director works best with Active Directory when its users are placed in global groups. Those global groups are then placed in the local groups of the Systems Director server.

For preferred practices, do not add Active Directory users directly to the local groups of any Systems Director servers.

4. Log in to the Systems Director web interface as an administrator and navigate to **Security** → **Users**. Active Directory users that are managed as a group do not appear in the list. However, you see the group. Users that are local to the Systems Director server show on this list because they are managed as individuals.

You can now assign additional roles to users to access specific Systems Director tasks and resources.

Authenticating LDAP users

Systems Director can authenticate user login requests to an LDAP server. In 3.7.5, “Lightweight Directory Access Protocol” on page 204, you can see an example of how to use LDAP for Systems Director.

3.7.2 Authorizing users

User authorization occurs when an authenticated user uses Systems Director to perform a task on a resource. The authorization mechanism compares the user account, or the group to which the user belongs, to the RBAC settings for that user or group. If a role exists that contains the necessary authorizations to complete that task on that specified resource, the task proceeds.

Users can access only the applications, tasks, and resources that their user accounts are authorized to access. The authorities that you grant to a user determine the console and resource information that the user can access, and the tasks that the user can perform on those resources.

Roles

You can assign roles to Systems Director users to control their access to resources and limit the tasks that they can perform on those resources. The authorities that you configure for a role determine the level of access that is granted to each user who is assigned to that role. All users or groups of users that access Systems Director must have a user role assignment.

The Systems Director server uses an RBAC service with which an administrator can create custom sets of permissions. The administrator assigns these sets of permissions, which are known as *roles*, to individual users or groups. An *authorization role* is a set of tasks, CLI commands, and application permissions that is applied to one or more resources. Each role can be applied to many users, and each user can have many roles. Regulating user roles is an effective way to control security for your system. By regulating user roles, you can control access to every task and CLI command.

The following roles are available in the Systems Director server by default:

- ▶ **SMAdministrator** (Administrator role)

The SMAdministrator role has full authority to perform all tasks and functions and full control over permissions. A user that is assigned to this role can perform all tasks

(including security administration, product installation, and configuration) with any resource.

► **SManager (Manager role)**

The SManager role can perform management operations, which are a subset of the functions that a member of the SAdministrator role can perform. Typically, system administration, system health management, and system configuration tasks are available. This role cannot perform security administration or security configuration tasks. However, this role has full access to all the Systems Director functions that are included in a functional manager or feature.

► **SMonitor (Monitor role)**

The SMonitor role can access the administrative functions that provide read-only access, such as monitoring, notification, and status. With this role, a user can complete tasks, such as monitoring a process, viewing and collecting inventory, and viewing hardware status.

► **SUser (User role)**

The SUser role includes any authenticated user and includes the ability to perform only basic operations, such as viewing resources and properties.

► **GroupRead (Group role)**

The GroupRead role has a single permission, which is known as group read, that defines the groups that are visible to each user. The administrator that assigns this role to a user can assign the groups that the user can view. The user then has access to see the groups but not necessarily the group contents.

These default user roles correspond directly with the groups that Systems Director installs at the operating system level. You cannot delete these roles and you cannot modify the permissions that are associated with them. However, you can add users and other groups to the system-defined roles as needed. You also can copy the system-defined roles or create new roles for your business needs.

Assigning a role to a user or user group

The roles that are assigned to a user or user group determine the tasks that the user has permission to access. From the Users page, you can assign one or more roles to a user or user group. When you assign a role, you also associate the specific resource groups to which that role applies to the selected user.

Before you can assign a role to a user, each user or group of users must have a valid user ID or group ID in the local operating system user registry on the management server. Also, ensure that the role that you want to assign to a user exists. If the role does not exist, you can create a role from the Roles page.

To assign a role to a user or group, complete the following steps:

1. In the Systems Director web interface navigation area, click **Security** → **Users and Groups**. Or, select **Manage Users** on the Home page Plug-ins tab. See Figure 3-87.

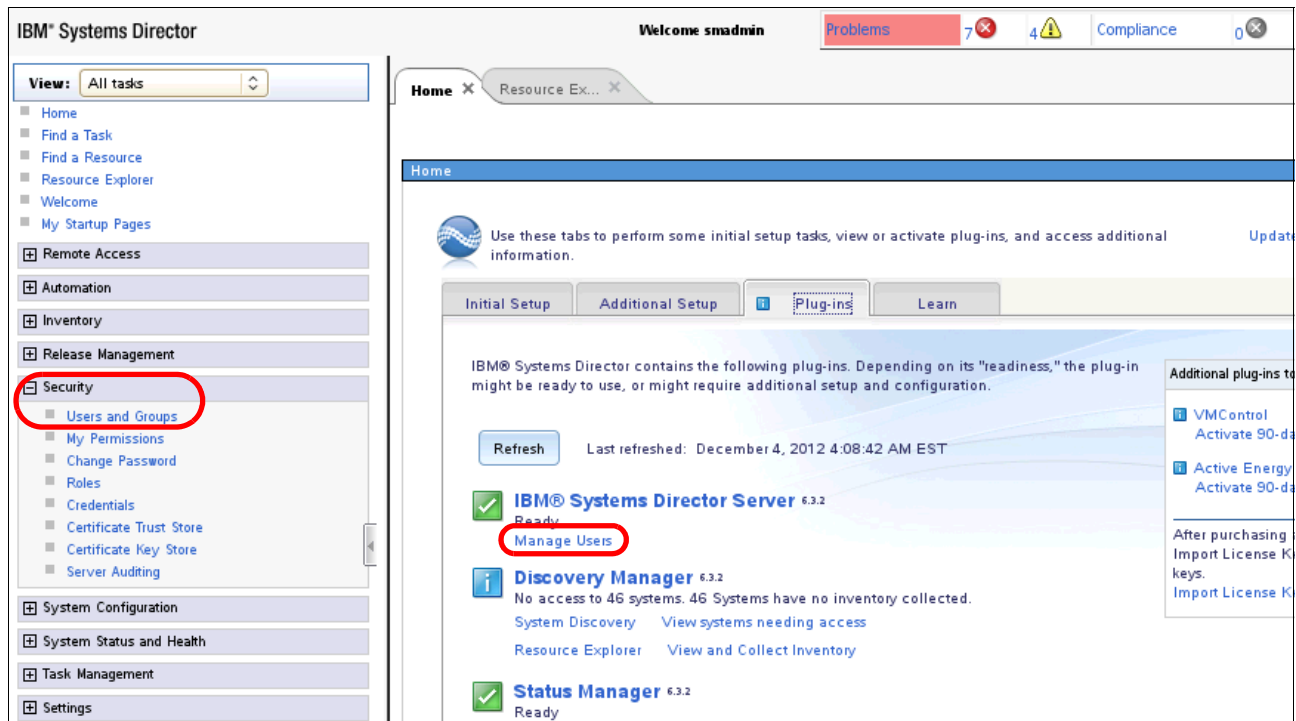


Figure 3-87 Security → Users and Groups or Manage Users

2. From the Users tab, select the user or group to which you want to assign a role. In our example, we select the user SMTtest (Figure 3-88).

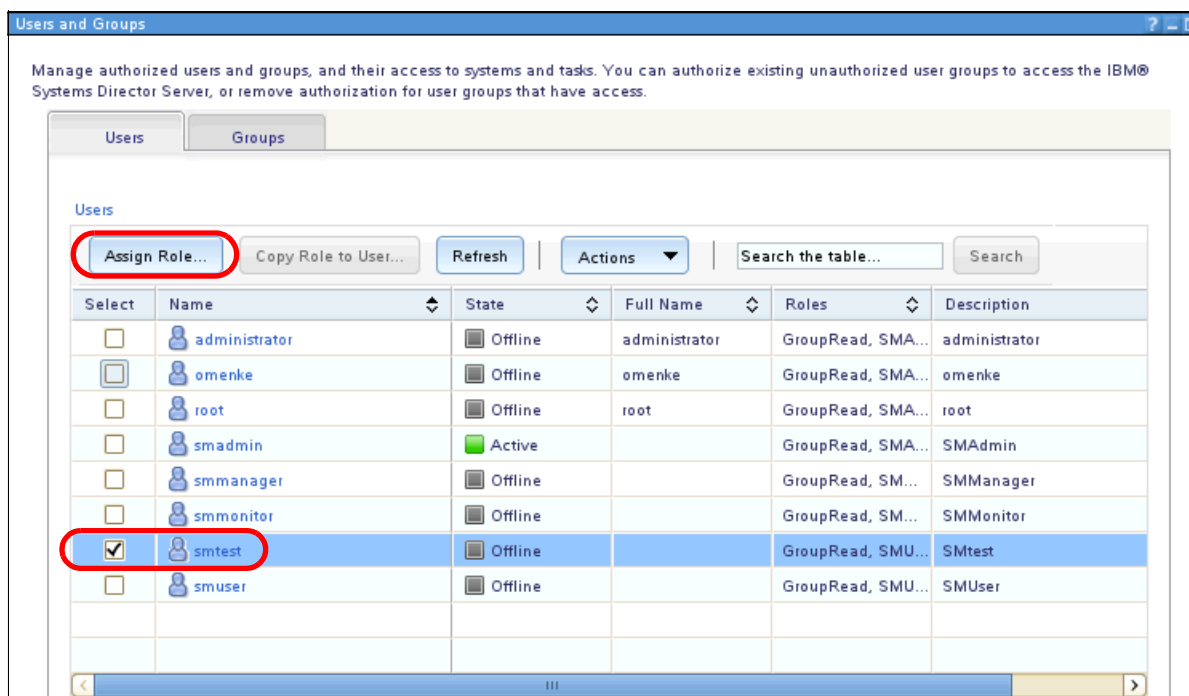


Figure 3-88 Select user for assigning role

3. Click **Assign Role**. The Welcome page for the Assign Role wizard opens (Figure 3-89). Click **Next**.

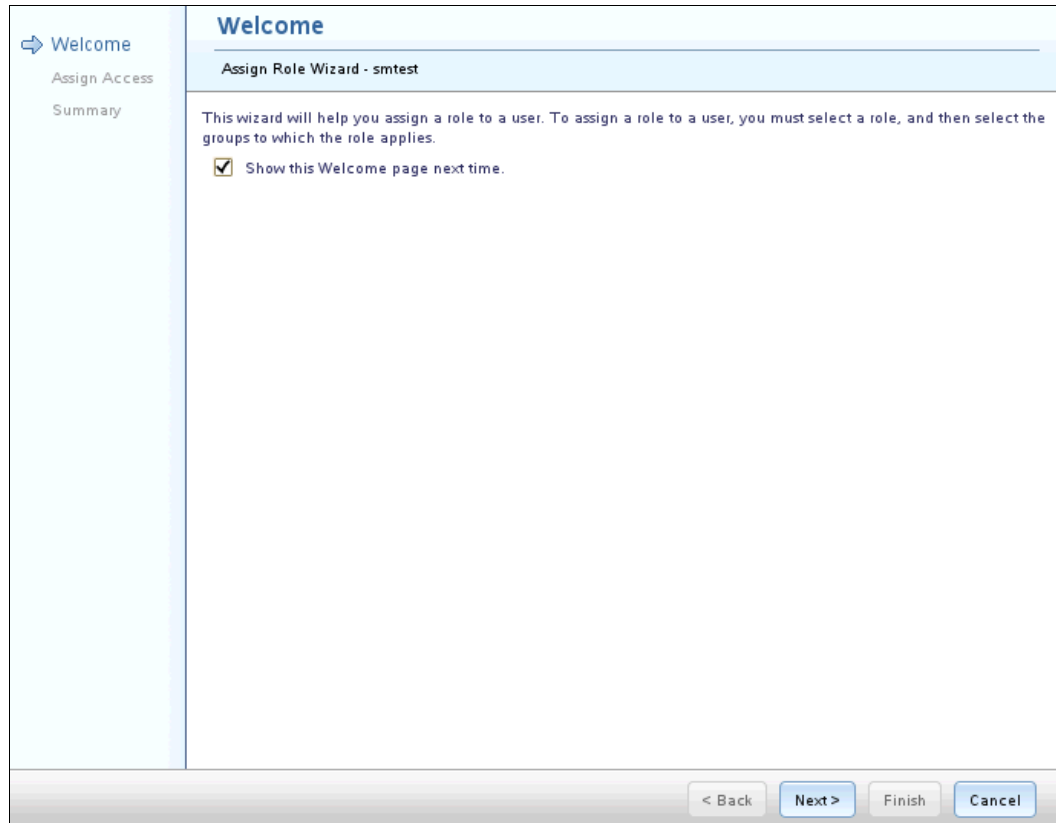


Figure 3-89 Welcome panel

4. The wizard lists the roles that are created. In our example, we select the SMMonitor role for the user SMTTest (Figure 3-90).

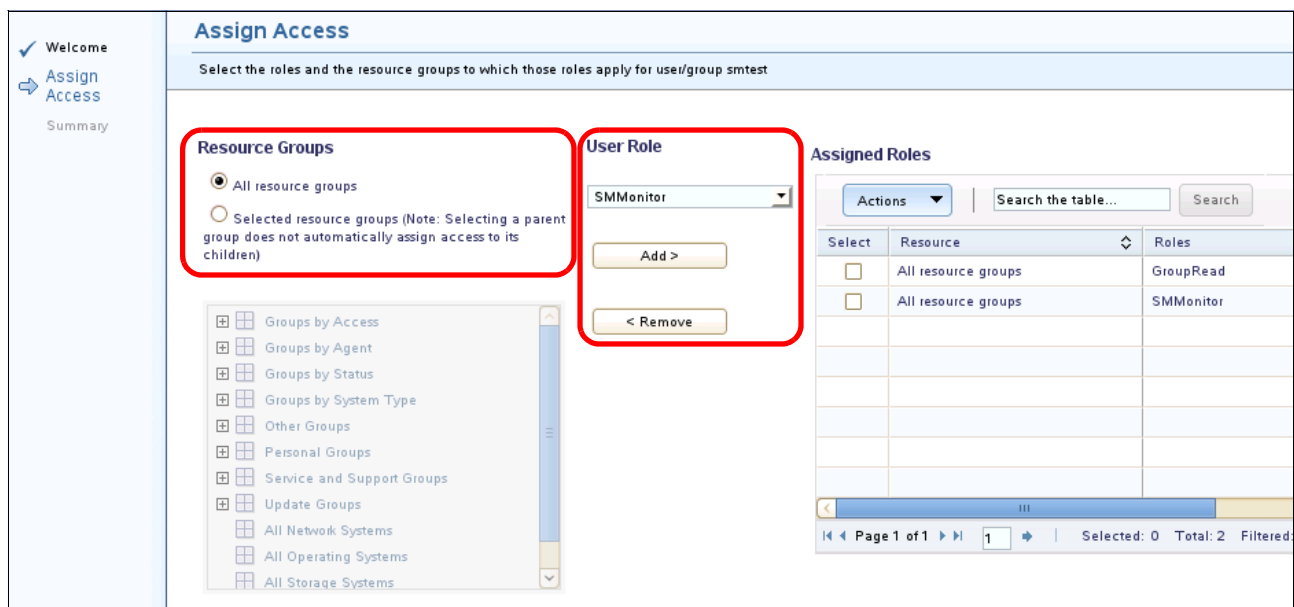


Figure 3-90 Assigning roles and resource groups

5. Select the role that you want to assign and click **Add**.
6. Select the resource groups that you want to associate with the role and the user. In our example, we select all Resource Groups.

Parent groups: Selecting a parent group does not automatically assign access to its children.

7. Click **Next**. The Summary page opens (Figure 3-91). Click **Finish**.



Figure 3-91 Summary page

Working with roles

Use Systems Director to work with roles and assign individual users and user groups to those roles. From the Roles page, you can view, copy, edit, or delete a role. To view, copy, edit, or delete a role, the role must exist. You can also use the Roles page to create a role that you can then manage.

Follow these steps to create a role:

1. In the navigation area, click **Security** → **Roles** (Figure 3-92).

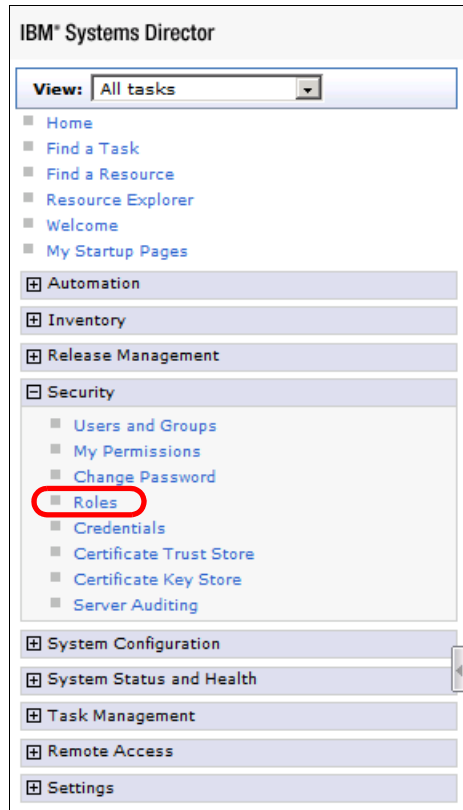


Figure 3-92 Select Roles from Security

2. On the Roles tab, click **Create** (Figure 3-93).

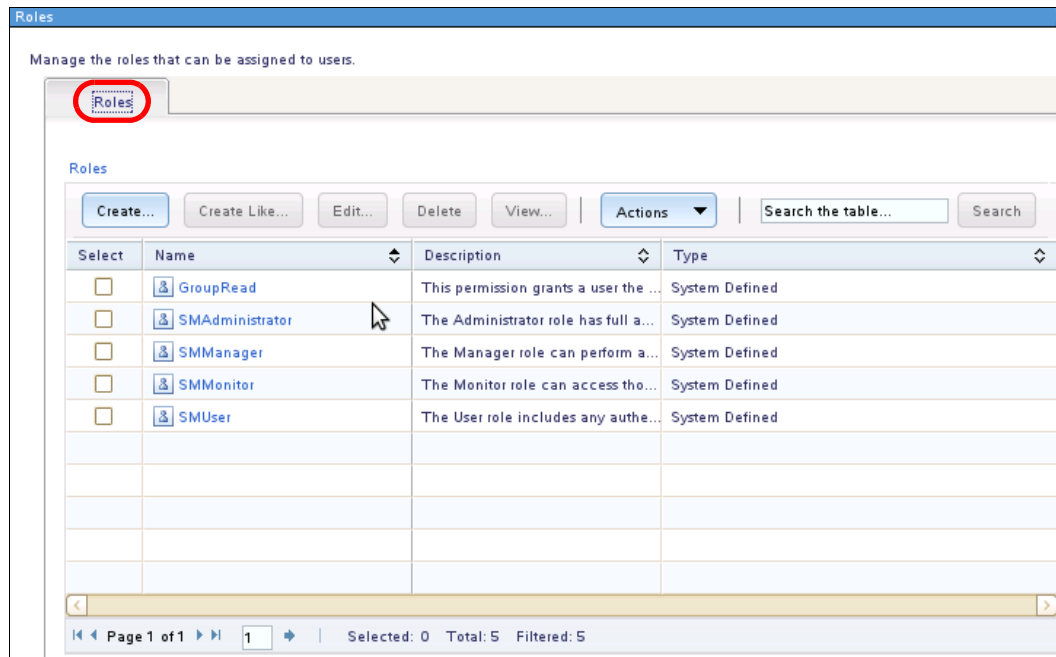


Figure 3-93 Create a role

3. The Create Role wizard Welcome page opens. Click **Next**.
4. The Name page opens (Figure 3-94). In the Name field, type a name for the role that you want to create. In our example, we named the new role book-Test. In the Description field, type an optional brief description for the role. Click **Next**.

The screenshot shows a wizard interface for creating a role. On the left, a vertical sidebar contains four items: 'Welcome' with a checkmark, 'Name' with a right-pointing arrow, 'Permissions', and 'Summary'. The main area is titled 'Name' and has a subtitle 'Specify a name and description for the role.' Below this, there are two input fields. The first is labeled '*Name:' and contains the text 'book-Test'. The second is labeled 'Description:' and contains the text 'Create Role for use in book'. A red circle is drawn around both input fields. At the bottom right of the main area, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 3-94 Naming the new role

5. The Permissions page opens (Figure 3-95 on page 200). In the Available permissions list, select a permission that you want to add to the user role and then click **Add**. The selected permission is added to the Selected permissions list. Continue to add permissions until you add all permissions that are required for the role.

In our example, we select Inventory and Task Management as permissions for the new role.

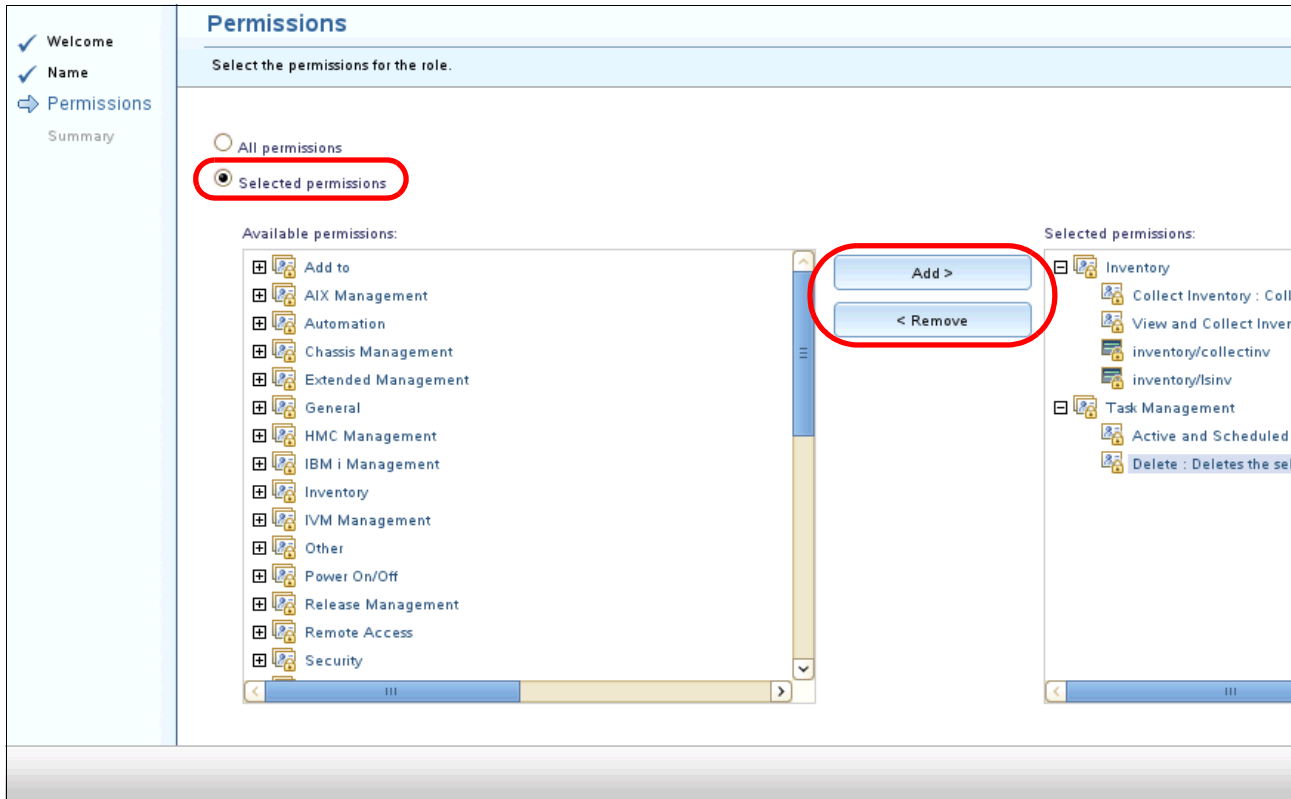


Figure 3-95 Select permissions

6. Click **Next**. The Summary page opens (Figure 3-96). Click **Finish**.

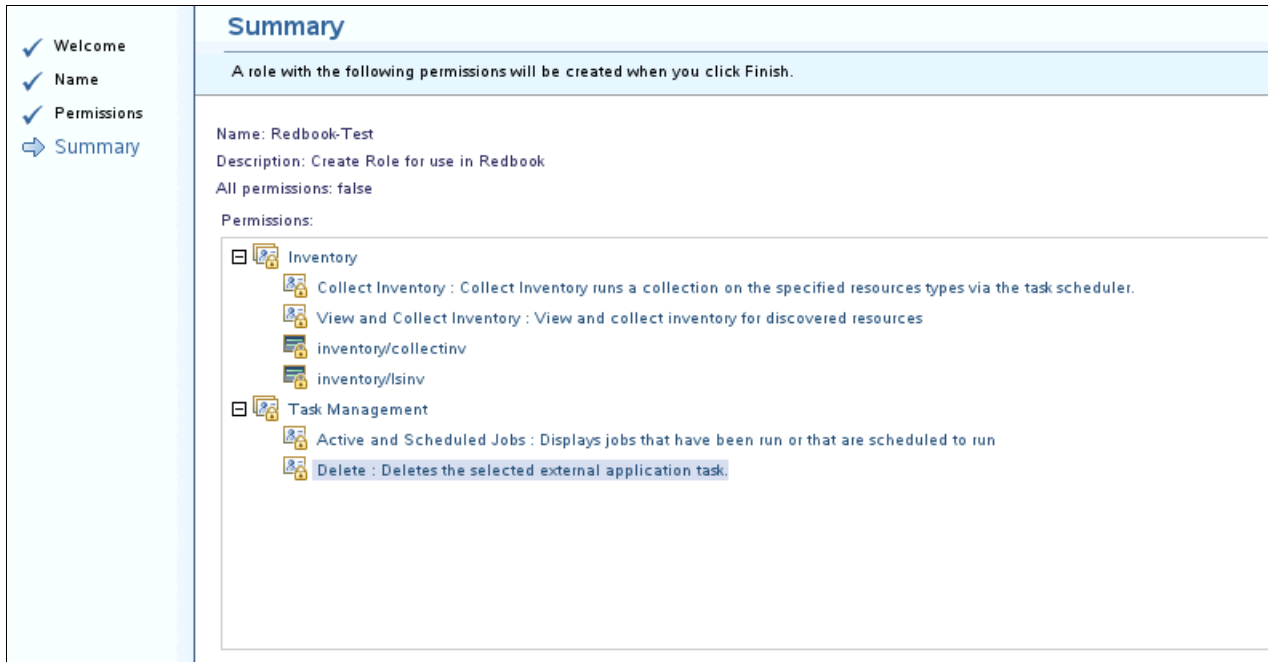


Figure 3-96 Summary page

3.7.3 Access managed systems

Use Systems Director to configure credentials that are used to access managed systems. These credentials enable Systems Director to authenticate to and manage target systems by using the available protocols and access points on the managed system.

You can request access to and configure access options for systems in your environment by using these tasks:

- ▶ Request access task
- ▶ Configure access task
- ▶ Configure system credentials task

You can also revoke access to an accessed system.

Security protocols

Depending on the managed system, the following communication protocols are supported (Figure 3-6).

Encrypted protocols: Not all protocols are encrypted as indicated in the table.

Table 3-6 Supported communication protocols

Managed system type	Communication protocol	Encrypted	Encryption algorithm
Agentless-managed system	Distributed component object model (DCOM)	Yes	RC2
	SNMP v1 and v2	No	None
	Secure Shell (SSH)	Yes	Encrypted algorithm is negotiated
Platform agent managed system	Agentless	Yes	Supports the communication protocols and encryption algorithms that are listed for the agentless-managed system
	Common Information Model (CIM)	Yes	If configured, encryption is enabled by default by using Secure Sockets Layer (SSL)
Common agent managed system	IBM Director 5.x interprocess communication (IPC)	Yes	AES, DES, or 3DES
	Tivoli Common Agent Services 6.x	Yes	SSL
Other	Service Location Protocol (SLP)	No	None

Access secured systems

Use the Request Access page to request access to a secured system if the management server to which you connect is not yet authenticated to the system. You must be able to access the system before you can perform tasks or remotely access the system.

Ensure that you have the correct authorization to access the secured system.

Secured systems are displayed in the Systems Director web interface with a padlock icon in the Access field or column of the system details (Figure 3-97). After a system is accessed, the padlock disappears and additional tasks and status information are available.

The Access attribute for each resource shows the current access status. You cannot request access to the resources with the following types of access status:

- ▶ Offline: Use verify access instead.
- ▶ OK: No further action is required. You already have access to these resources.

To request access to secured managed systems, complete the following steps:

1. In the Systems Director web interface, click **Resource Explorer**.
2. Navigate to the system that you want to access.
3. Right-click the system for which you want to request access and click **Security** → **Request Access**.

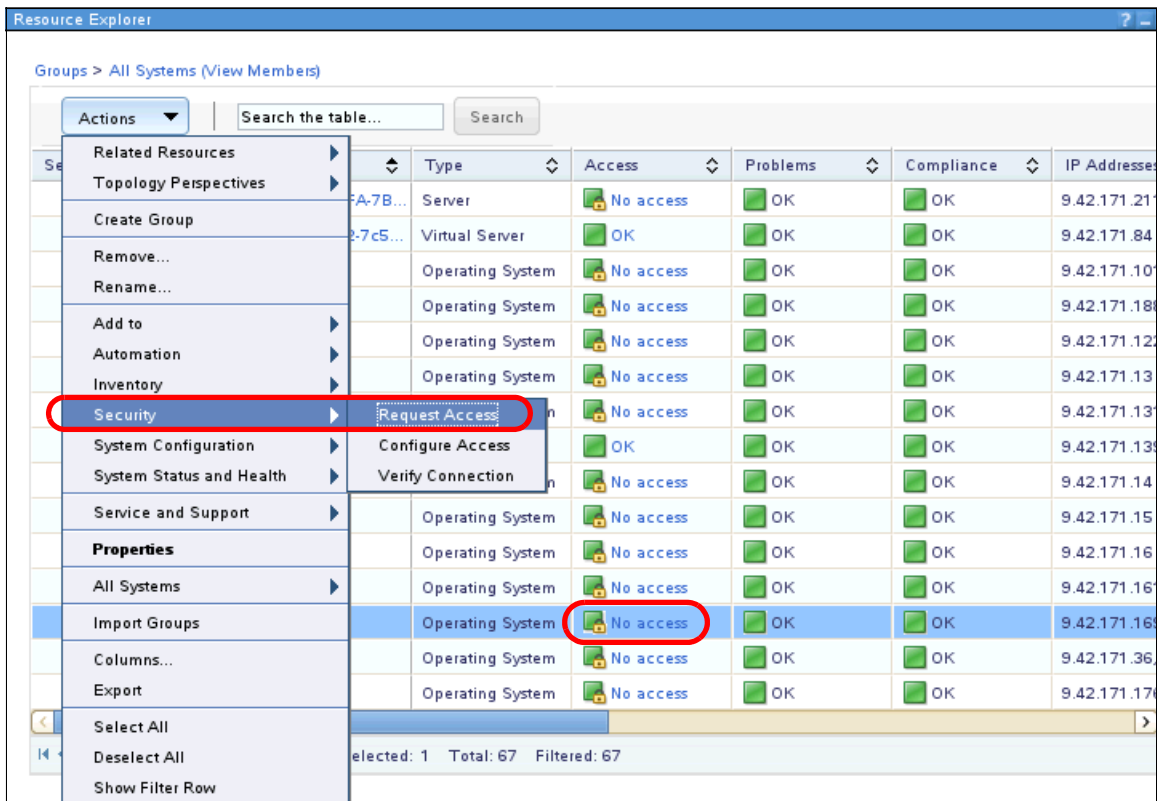


Figure 3-97 Request Access

Tip: Alternatively, you can click **Security** → **Configure Access** and then click **Request Access** on the Configure Access page.

4. On the Request Access page, type the user ID and password of a user that belongs to the System group (Figure 3-98). Only certain user accounts can be used to request access.

Request Access

Specify the user ID and password to authenticate Systems Director to one or more target systems. Then click Request Access to grant all authorized Systems Director users access to the target system(s).

*User ID:
Administrator

*Password:

Request Access Close

Selected targets:

Name	Access	Trust State
9.42.171.169	No access	Not applicable

Page 1 of 1 Total: 1

Figure 3-98 Request Access

The following list shows the detailed requirements of the user accounts that can be used to request access for various types of agent systems:

- Common Agent:
 - Linux/AIX: Root or user in the system group
 - Windows: Administrator or user in the administrator group
- Platform Agent:
 - Linux/AIX: Root or user in the system group
 - Windows: Administrator or user in the administrator group
- Agentless systems:
 - Linux/AIX: Root or user in the system group. User that is configured with the **sudo** command.
 - Windows: Administrator or user in the administrator group

Click **Request Access**. Credentials are created and authenticated to the managed system in an attempt to access it. If the access request is successful, the access status for the managed system changes to OK.

If the access status changes to Partial Access, the access request was unsuccessful for at least one protocol. Click **Configure Access** to see the list of available protocols for the system and their access states. If necessary, to create additional credentials, click an access point that does not have an access state of OK and repeat this procedure.

For information about accessing systems by using credentials, configuring access, or accessing CIM systems by using the x509 certificate, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_t_managing_access.html

3.7.4 Credentials

The Systems Director server uses credentials to implement single sign-on (SSO) authentication. By using SSO with this authentication process, a user can access more than one system or application by entering a single user ID and password. The Systems Director server maps web interface user credentials to the necessary user credentials for authenticating to the target managed system. These credentials are saved in registries.

It is a preferred practice to use SSO because users are not required to type the user ID and password for the target system or resource each time that they or tasks access it. The Systems Director server automatically logs on as needed by retrieving the necessary credentials.

There are two types of credentials:

- ▶ Shared credentials

Shared credentials are those credentials that exist in an authentication registry that is not specific to an access point.

- ▶ Targeted credentials

Targeted credentials are each assigned to only one remote-service agent access point and are in an authentication registry that is specific to that access point.

For more information about credentials, see the Systems Director Information Center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_c_credentials.html

3.7.5 Lightweight Directory Access Protocol

The Systems Director server can authenticate users that are defined in the LDAP directory. Many benefits are possible if you use LDAP as the preferred authentication method:

- ▶ Ease of management
- ▶ Central administration
- ▶ Cross-platform synergies

The following LDAP servers are supported by Systems Director:

- ▶ Microsoft Active Directory
- ▶ IBM Lotus® Domino®
- ▶ IBM Tivoli Director Server
- ▶ Sun One
- ▶ OpenLDAP
- ▶ IBM Secure Way Server
- ▶ Novell eDirectory

Configuring OpenLDAP

We configure OpenLDAP on Red Hat Enterprise Linux Server 5.6. Install the Red Hat Package Manager (RPM) packages that are shown in Figure 3-99.

```
[root@xs-2120rhelppc ~]# rpm -qa | grep openld
compat-openldap-2.3.43_2.2.29-12.e15_5.3
openldap-devel-2.3.43-12.e15_5.3
openldap-2.3.43-12.e15_5.3
openldap-clients-2.3.43-12.e15_5.3
openldap-servers-2.3.43-12.e15_5.3
openldap-2.3.43-12.e15_5.3
openldap-devel-2.3.43-12.e15_5.3
[root@xs-2120rhelppc ~]
```

Figure 3-99 OpenLDAP RPM packages

Discuss the properties that need to be edited in the `securityLDAP.properties` file with your LDAP administrator. For more information about LDAP, see the information center at the following link:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_t_ldap_authentication.html

File name change: Rename the `security.ldap` file to the `securityLDAP.properties` file after you change the properties. If you use LDAP, Systems Director looks for the `securityLDAP.properties` file.

Table 3-7 shows the properties to be referenced or changed in the `securityLDAP.properties` file.

Table 3-7 OpenLDAP securityLDAP.properties file properties to change

Property	Value	Description
<code>com.ibm.lwi.LDAPHost</code>	IP or hostname	Address of LDAP server
<code>com.ibm.lwi.LDAPAdminPassword</code>	Encrypted password	Read-only password for binding
<code>com.ibm.lwi.LDAPBase</code>	<code>dc=itso,dc=ibm</code>	Base distinguished name (DN) for LDAP server
<code>com.ibm.lwi.searchfilter</code>	<code>(&(uid=%v)(objectclass=inetOrgPerson))</code>	The user search filter for the LDAP server
<code>com.ibm.lwi.rolemanager.ldap.filters.usergroup</code>	<code>(objectclass=posixGroup)</code>	Authorized groups for the Systems Director server
<code>com.ibm.lwi.rolemanager.ldap.filters.users</code>	<code>(!(objectClass=inetOrgPerson)(objectClass=posixAccount))</code>	Group objects search
<code>com.ibm.lwi.rolemanager.ldap.names.memberAttribute</code>	<code>uid</code>	Member attribute role object
<code>com.ibm.lwi.rolemanager.ldap.names.loginName</code>	<code>uid</code>	Name of login attribute of user
<code>com.ibm.lwi.rolemanager.ldap.names.groupID</code>	<code>gidNumber</code>	Name of the group ID attribute of the group object
<code>com.ibm.lwi.rolemanager.ldap.names.userPrimaryGroupID</code>	<code>gidNumber</code>	Name of the group ID attribute of the group object

Property	Value	Description
com.ibm.lwi.rolemanager.ldap.filters.usersByGroupId	(&(gidNumber={0})(!(objectClass=inetOrgPerson)(objectClass=posixAccount)))	Users by gidNumber or member
com.ibm.lwi.rolemanager.ldap.filters.groupsByMembers	(&(gidNumber={0})(memberUid={1})(objectclass=posixGroup))	Groups by gidNumber or posixGroup
com.ibm.lwi.rolemanager.ldap.names.memberAttribute.isDN	false	Specific to openLDAP

For information about the OpenLDAP slapd server configuration, see the following Red Hat web page:

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/4/html/Reference_Guide/s1-ldap-quickstart.html#s2-ldap-files-slapd-conf

After you successfully install the required RPM packages, configure the `slapd.conf` file and encrypt the rootpw password by using the `slappasswd` command as shown in Figure 3-100.

```
[root@xs-2120rhelppc openldap]# slappasswd
New password:
Re-enter new password:

{SSHA}4eb+Hf7KScsth8vftJ/Fdw8jKXV+mRL
```

Figure 3-100 `slappasswd`

The following configuration changes for the `slapd.conf` file are shown in Figure 3-101:

- ▶ suffix
- ▶ rootdn
- ▶ rootpw

```
database          bdb
suffix            "dc=itso,dc=ibm"
rootdn            "cn=root,dc=itso,dc=ibm"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw          secret
rootpw {SSHA}4eb+Hf7KScsth8vftJ/Fdw8jKXV+mRL
```

Figure 3-101 `slapd.conf` file configuration changes

From the command line, start the LDAP service and add an entry to start the service automatically on boot by using `chkconfig` as shown in Figure 3-102.

```
[root@xs-2120rhelppc openldap]# service ldap start
Checking configuration files for slapd:  config file testing succeeded
                                         [ OK ]
Starting slapd:                          [ OK ]
[root@xs-2120rhelppc openldap]# chkconfig ldap on
[root@xs-2120rhelppc openldap]# chkconfig --list | grep ldap
ldap          0:off  1:off  2:on   3:on   4:on   5:on   6:off
[root@xs-2120rhelppc openldap]#
```

Figure 3-102 Service start: `chkconfig` check

Importing groups and users

From the LDAP server command line, import the ldif files for users and groups. To complete this task, we create a ldif file for importing. Create a groups.ldif file as shown in Figure 3-103.

```
dn: cn=smadmin,dc=itso,dc=ibm
cn: smadmin
objectClass: top
objectClass: posixGroup
gidNumber: 100
memberUid: root
memberUid: uid=root,cn=smadmin,dc=itso,dc=ibm

dn: uid=root,cn=smadmin,dc=itso,dc=ibm
cn: root
sn: root
uid: root
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 100
gidNumber: 100
homeDirectory: /root
userPassword: operah09se

dn: cn=smmon,dc=itso,dc=ibm
cn: smmon
objectClass: top
objectClass: posixGroup
gidNumber: 101
memberUid: isduser
memberUid: uid=isduser,cn=smmon,dc=itso,dc=ibm

dn: cn=smmgr,dc=itso,dc=ibm
description: smmgr
cn: smmgr
objectClass: top
objectClass: posixGroup
gidNumber: 102
memberUid: uid=isdmgr,cn=smmgr,dc=itso,dc=ibm
memberUid: uid=isdmgr0,cn=smmgr,dc=itso,dc=ibm

dn: cn=smuser,dc=itso,dc=ibm
description: smuser
cn: smuser
objectClass: top
objectClass: posixGroup
gidNumber: 103
```

Figure 3-103 groups.ldif file

Create a users.ldif file as shown in Figure 3-104.

```
dn: uid=isduser,cn=smmn,dc=itso,dc=ibm
cn: isduser
sn: isduser
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
uid: isduser
uidNumber: 101
gidNumber: 101
homeDirectory: /home/isduser
userPassword: @Pa22w0rd

dn: uid=isdmgr0,cn=smmgr,dc=itso,dc=ibm
cn: isdmgr0
sn: isdmgr0
uid: isdmgr0
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 102
gidNumber: 102
homeDirectory: /home/isdmgr0
userPassword: @Pa22w0rd

dn: uid=isdmgr1,cn=smmgr,dc=itso,dc=ibm
cn: isdmgr1
sn: isdmgr1
uid: isdmgr1
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 103
gidNumber: 102
homeDirectory: /home/isdmgr1
userPassword: @Pa22w0rd
```

Figure 3-104 users.ldif file

The two ldif files are imported by using the ldapadd file as shown in Figure 3-105.

```
[root@xs-2120rhelppc ldapFiles]# ldapadd -H ldap://127.0.0.1 -x -D
"cn=root,dc=itso,dc=ibm" -f ~/ldapFiles/groups.ldif -w @Pa22w0rd
adding new entry "cn=smadmin,dc=itso,dc=ibm"

adding new entry "uid=root,cn=smadmin,dc=itso,dc=ibm"

adding new entry "cn=smon,dc=itso,dc=ibm"

adding new entry "cn=smmgr,dc=itso,dc=ibm"

adding new entry "cn=smuser,dc=itso,dc=ibm"

[root@xs-2120rhelppc ldapFiles]# ldapadd -H ldap://127.0.0.1 -x -D
"cn=root,dc=itso,dc=ibm" -f ~/ldapFiles/users.ldif -w @Pa22w0rd
adding new entry "uid=isduser,cn=smon,dc=itso,dc=ibm"

adding new entry "uid=isdmgr0,cn=smmgr,dc=itso,dc=ibm"

adding new entry "uid=isdmgr1,cn=smmgr,dc=itso,dc=ibm"
```

Figure 3-105 ldapadd file

To view the LDAP server, we use the LDAP command line (Figure 3-106).

```
[root@xs-2120rhelppc openldap]#ldapsearch -x -b 'dc=itso,dc=ibm'
# extended LDIF
#
# LDAPv3
# base <dc=itso,dc=ibm> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# itso.ibm
dn: dc=itso,dc=ibm
dc: itso
o: itso
objectClass: organization
objectClass: dcObject
# smadmin, itso.ibm
dn: cn=smadmin,dc=itso,dc=ibm
cn: smadmin
objectClass: top
objectClass: posixGroup
gidNumber: 100
memberUid: root
memberUid: uid=root,cn=smadmin,dc=itso,dc=ibm
# root, smadmin, itso.ibm
dn: uid=root,cn=smadmin,dc=itso,dc=ibm
cn: root
sn: root
uid: root
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 100
gidNumber: 100
homeDirectory: /root
userPassword:: b3B1cmFoMD1zZQ==
# smmon, itso.ibm
dn: cn=smmon,dc=itso,dc=ibm
cn: smmon
objectClass: top
objectClass: posixGroup
gidNumber: 101
memberUid: isduser
# smmgr, itso.ibm
dn: cn=smmgr,dc=itso,dc=ibm
description: smmgr
cn: smmgr
objectClass: top
objectClass: posixGroup
gidNumber: 102
memberUid: uid=isdmgr,cn=smmgr,dc=itso,dc=ibm
memberUid: uid=isdmgr0,cn=smmgr,dc=itso,dc=ibm
memberUid: uid=isdmgr1,cn=smmgr,dc=itso,dc=ibm
```

Figure 3-106 *ldapsearch*

The LDAP server is now ready. The groups are defined. The users are defined. And, the securityLDAP.properties file is configured. Therefore, we can make the last changes to the Systems Director server so that we can start to use LDAP as its authentication method (Figure 3-107).

```
-bash-3.2# cd /opt/ibm/director/lwi/conf/overrides/  
-bash-3.2# mv security.ldap securityLDAP.properties  
-bash-3.2# mv security.properties security.properties.old  
-bash-3.2# smstop;smstart;smstatus -r
```

Figure 3-107 File changes

From the Systems Director server home page, click **Plug-ins** and then **IBM Systems Director Server**. A summary window opens and the authentication type is listed (Figure 3-108). The configuration is successful.



Figure 3-108 Confirming that LDAP is successfully configured

We now use OpenLDAP as the authentication type.

Important: This example is a basic setup of openLDAP. Ensure that you take additional security measures with your configuration to further secure the openLDAP server and LDAP administration.

Authenticating users and groups

Additional groups and their associated users can be authorized to Systems Director. This authorization can be set up for new groups or groups that exist in the LDAP domain.

The following example imports a new Systems Director group with users to the OpenLDAP server by using the `ldapadd` command. This group is called the `isdgroup` (Figure 3-109).

```
[root@xs-2120rhelppc ldapFiles]# ldapadd -H ldap://127.0.0.1 -x -D
"cn=root,dc=itso,dc=ibm" -f ~/ldapFiles/addgroup.ldif -w operah09se
adding new entry "cn=isdgroup,dc=itso,dc=ibm"

[root@xs-2120rhelppc ldapFiles]# ldapadd -H ldap://127.0.0.1 -x -D
"cn=root,dc=itso,dc=ibm" -f ~/ldapFiles/adduser.ldif -w operah09se
adding new entry "uid=user0,cn=isdgroup,dc=itso,dc=ibm"

adding new entry "uid=user1,cn=isdgroup,dc=itso,dc=ibm"
```

Figure 3-109 Authorizing an additional group

Now that the group is added, we add the additional users because this task is an incremental installation. Then, we need to authorize the group to Systems Director. Follow these steps:

1. From the Systems Director home page, click **Security** → **Users and Groups** → **Groups**. Then, click **Authorize Groups**. The Authorize User Groups wizard starts.
2. On the Welcome page, click **Next**.
3. Figure 3-110 appears. The group that was imported to LDAP by using the `ldapadd` command is displayed. Place a check mark next to the group and click **Next**.

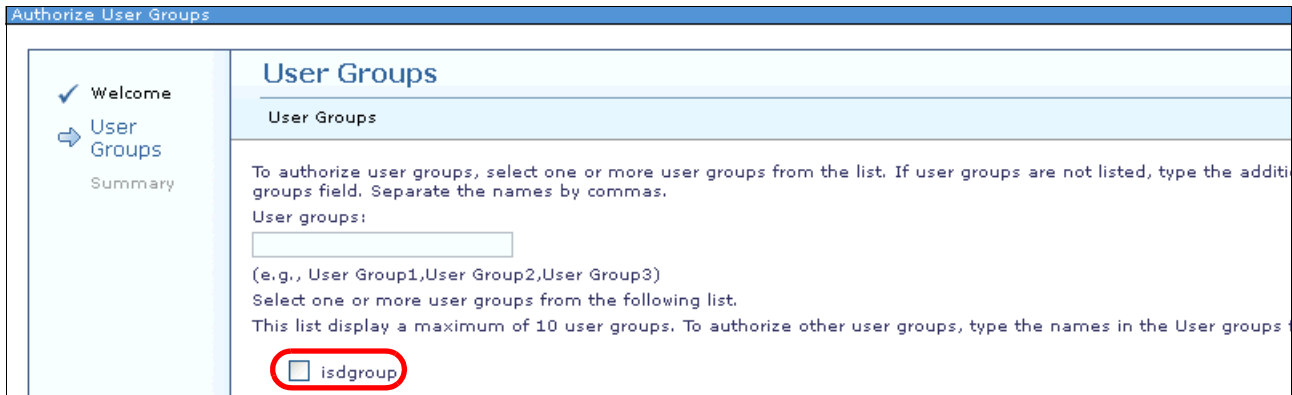


Figure 3-110 Authorize User Groups

4. Click **Finish** to authorize the `isdgroup` user group and complete the wizard.

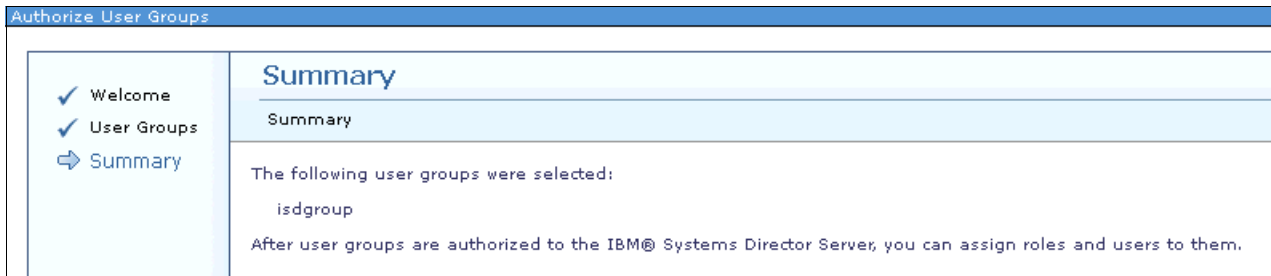


Figure 3-111 Authorize the `isdgroup` user group

5. We still need to assign a role to the group that is authorized. The group can be assigned to a custom role or one of the default roles:
 - SMAAdministrator

- SMManager
- SMMonitor
- SMUser

6. Select the group that we authorized (note that Roles is empty for the isdgroup group in Figure 3-112) and click **Assign Role**.



Figure 3-112 Assign Role

7. For this group, we assign an SMAdministrator role to the group. The Assign Role wizard starts. Click **Next**.

8. Then, on the Assign Role window (Figure 3-113), choose **SMAdministrator** from the pull-down menu that is highlighted in Figure 3-113 and **Add**.

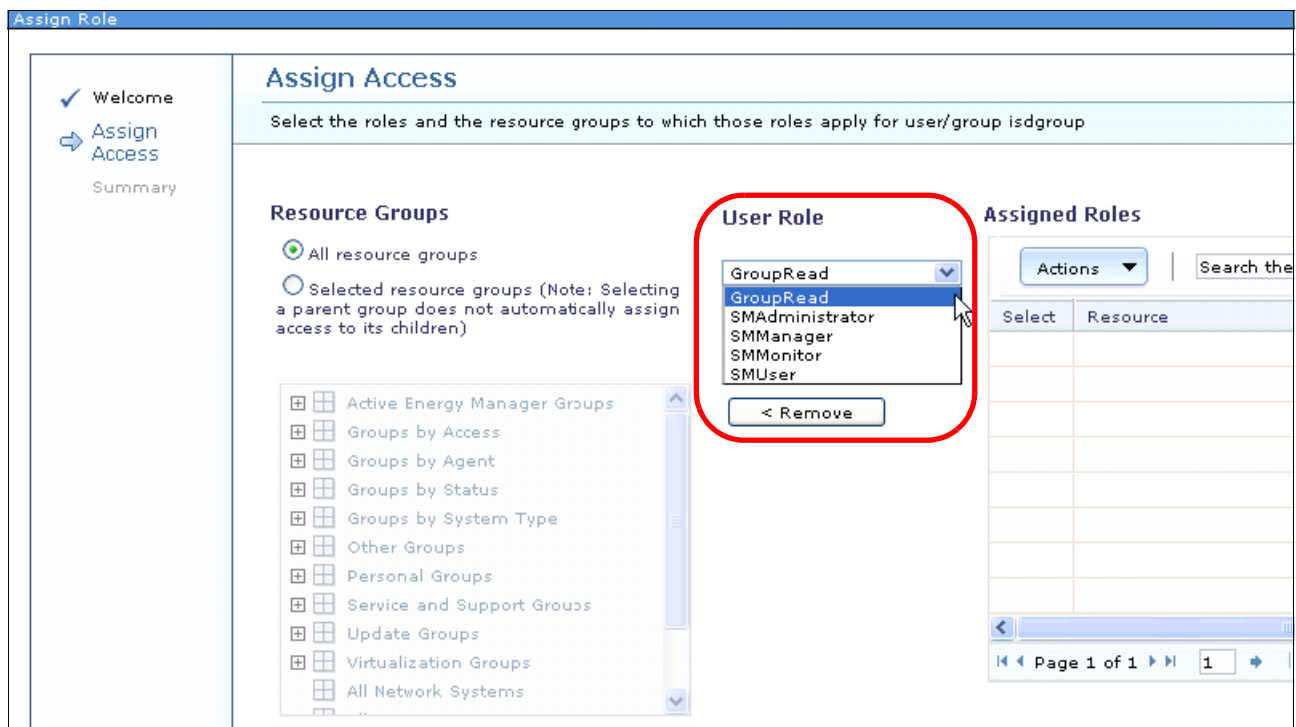


Figure 3-113 Assign Role

9. On completion, click **Next** and **Finish**.

10. Now, the `isdgroup` group and its associated users have `SMAAdministrator` access to all resources.

11. From the home page, click **Security** → **Users and Groups** → **Users** (Figure 3-114).

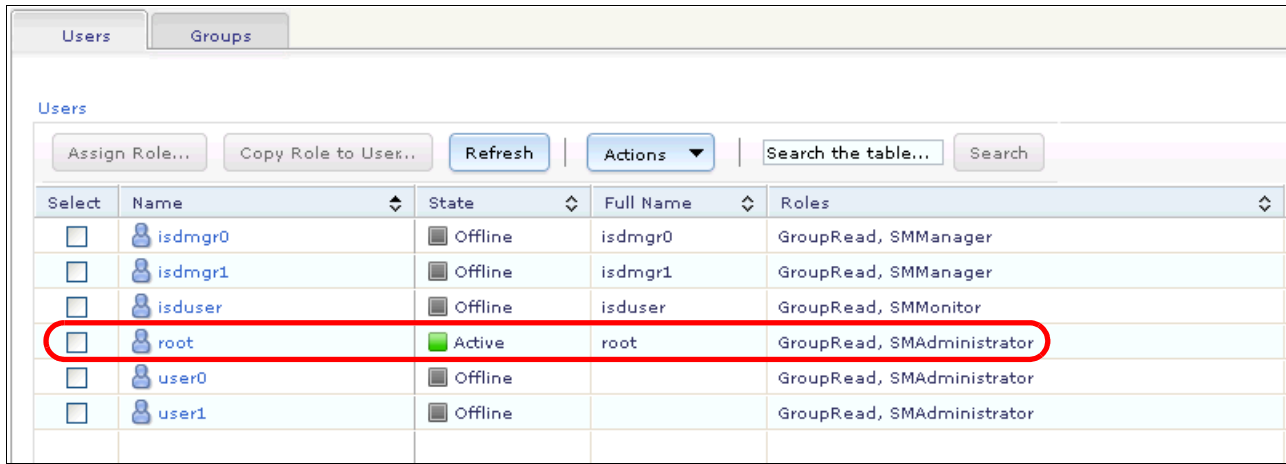


Figure 3-114 User listing

You can now successfully log on as a user that is listed in the `isdgroup`.

Tip: When you use the wizard to authorize groups, only the first 10 groups are returned in Figure 3-111. If your group is not listed, type the name. If the typed name does not return the group, check your filters in the `securityLDAP.properties` file.

3.7.6 Using command-line tools for security

There are many available `smcli` command-line tools for security settings as listed in Table 3-8.

Table 3-8 Command-line tools for security

Command	Description
<code>authusergp</code>	Authorize an existing user group to access the Systems Director server.
<code>cfgaccess</code>	Configure access for systems that are managed by Systems Director.
<code>cfgappcred</code>	Change the password that Systems Director uses to access particular associated applications.
<code>cfgcertpolicy</code>	View or configure the trust management certificate policy that IBM Systems Director uses.
<code>cfgcred</code>	Configure credentials for systems that are managed by Systems Director.
<code>cfgpwdpolicy</code>	Manage the password policies of users that Systems Director creates or manages.
<code>chaudit</code>	Modify audit settings.
<code>chcred</code>	Change credentials for systems that are managed by Systems Director.
<code>chrole</code>	Change the properties of a role.
<code>chuser</code>	Modify the properties of a user.
<code>chusergp</code>	Change attributes and access privileges for a user group.

Command	Description
exportcert	Export a certificate from a Systems Director keystore or truststore to a .pem file.
importcert	Import certificates into a Systems Director keystore or truststore.
lsaudit	List audit settings and categories.
lsauditlogs	List a specific number of audit log messages for one or more audit categories.
lscert	List the certificates in a Systems Director keystore or truststore.
scred	List credentials for systems that are managed by Systems Director.
lspem	List the permissions.
lsrole	List the roles in Systems Director.
lsuser	List users.
lsusergp	List the Systems Director user groups.
mkrole	Create roles that contain a list of permissions for authorization to access Systems Director.
revokecert	Invalidate certificates in a Systems Director keystore or truststore.
rmauditlogs	Remove the audit log for one or more audit categories.
rmcert	Remove certificates from a Systems Director keystore or truststore.
rmcred	Remove credentials for systems that are managed by Systems Director.
rmrole	Delete roles.
rmusergp	Remove the access authorization for a user group or remove a user group.
unrevokecert	Revalidate revoked certificates in a Systems Director keystore or truststore.

For detailed information about the commands and all options for these commands, see the information center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_r_roles_required_to_run_commands.html

Accessing command-line tools by role/group

The command-line tools are restricted by the permissions. Table 3-9 lists which commands can be accessed by the roles.

Table 3-9 Command-line tools by role/group

Group	Restricted	Specifics
SMAdmin	Unrestricted	All commands
SManager	Restricted	All commands except the security and system commands
SMMonitor	Restricted	All commands with list functions, such as lscfgplan , lsinv , lsled , lsstatus , lsresmon , and lsevtfltr Also, commands, such as checkupd and lsupd , or commands for SNMP, such as get , walk , and getnext
SMUser	Restricted	Only support for the following commands: lssys , lsgp , lsjob , lsjobhistory , lstask , runjob , and runtask

For a complete list, see this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.security.helps.doc%2Ffqm0_r_roles_required_to_run_commands.html

3.7.7 Error logs and troubleshooting

If you are unable to log on to the Systems Director server or if the server fails to start, review the logs to determine the error. You can increase the logging with Systems Director in two ways:

- ▶ **lwi log.sh** script
- ▶ `logging.properties` file

If the server is active, use the **lwi log.sh** script as shown in Figure 3-115.

```
-bash-3.2# /opt/ibm/director/lwi/bin/lwi log.sh -addlogger -name
com.ibm.lwi.security.rolemanagers.ldap -level FINEST
ALR0299I: Logger successfully added for package com.ibm.lwi.security.rolemanagers.ldap.
SUCCESS
-bash-3.2
```

Figure 3-115 `lwi log.sh` script

If the server is not active, edit the `logging.properties` file as shown in Figure 3-116.

```
-bash-3.2#echo -e "#additional LDAP
logging\com.ibm.lwi.security.rolemanagers.ldap.level=FINEST"
>>logging.properties
```

Figure 3-116 Increase the logging level

The following additional logging attributes are available:

- ▶ For the **lwi log.sh** script:
 - `com.ibm.usmi.kernel.security -level FINEST`
 - `com.ibm.usmi.console.security -level FINEST`
- ▶ For the `logging.properties` file:
 - `com.ibm.usmi.kernel.security.level=ALL`
 - `com.ibm.usmi.console.security.level=ALL`

After the logging threshold is changed by using the **lwi log.sh** script, refresh the logs by using the **-refresh** parameter:

```
/opt/ibm/director/lwi/bin/lwi log.sh -refresh
```

If you edit the `logging.properties` file, restart the Systems Director server. Log files are stored in the `/opt/ibm/director/lwi/logs/error-log-0.html` directory.

Restoring local OS authentication

To restore Systems Director to use local OS authentication, use the **cfguserreg.sh** script (Figure 3-117). Before you use the script, restore the original `security.properties` file.

Remove the securityLDAP.properties file from the /opt/ibm/director/lwi/conf/overrides/ directory.

```
-bash-3.2# cfguserreg.sh -os
/opt/ibm/director/bin
Security settings have been set to use operating system registry.
Restart IBM Systems Director Server to complete configuration.

-bash-3.2#smstop;smstart;smstatus -r
Shutting down IBM Director...
Starting IBM Director...
The starting process may take a while. Please use smstatus to check if the server is
active.
Starting
Active
```

Figure 3-117 *cfguserreg.sh*

Additional information

For OpenLDAP support with Systems Director, see the IBM Support Portal:

<http://ibm.com/support/search.wss?q1=openldap&tc=SGZ2Z3>

For common troubleshooting steps with LDAP, see this website:

<http://ibm.com/support/docview.wss?uid=nas7917752a664b2c71a8625768e0001ab13>

For additional common troubleshooting steps with LDAP, see this website:

<http://ibm.com/support/docview.wss?uid=nas7cf1a05b97228ef0d86257749007b7025>



Backup

Why to back up the IBM Systems Director server and how to recover from a Systems Director failure are described.

The following topics are included:

- ▶ 4.1, “Backup Q&A” on page 220
- ▶ 4.2, “Backup and recovery” on page 220
- ▶ 4.3, “Migration” on page 225

4.1 Backup Q&A

You might ask the following backup questions:

▶ Why back up?

Backing up the Systems Director, including all data and settings, makes it easier to recover from a Systems Director server crash. Systems Director provides command-line tools to perform both the backup and the recovery. These tools are explained in 4.2, “Backup and recovery” on page 220.

▶ When do I back up?

The preferred practice is to back up your Systems Director server after installation and initial configuration. Also, back up after discovery and inventory but before you first install any updates. Then, you can quickly recover back to a fresh installation, if necessary. Always back up after you make any updates to the Systems Director server.

▶ How often do I back up?

We suggest that you back up before you install plug-ins or advanced managers. We also recommend that you back up regularly, such as once a month.

▶ What information is backed up?

▶ The Systems Director backup routine creates a backup image of Systems Director persistent data. *Persistent data* includes file system data, which is also called *master data*, and database data:

- Information about discovered systems and their access state
- All event automation plans
- All groups
- All inventory data that is stored in the Systems Director database
- Event logs

The backup also includes data in the local repository, such as updates that you downloaded.

▶ What can the backup not be used for?

Do not use the backup procedures to migrate to a new version or to switch over to another system with another version of Systems Director or another database. For a migration, use other tools that are described in 4.3, “Migration” on page 225.

4.2 Backup and recovery

To protect your Systems Director 6.3.x data from a disaster, back up and restore your data. Use commands that are provided by Systems Director.

The following command-line tools are used for backup and recovery:

- ▶ **smsave** (backup)
- ▶ **smrestore** (restore)
- ▶ **smreset** (reset)

4.2.1 Systems Director backup

Use the **smsave** command to save a backup image of the Systems Director server. The command is in the `install_root\bin\` directory, where `install_root` is the root directory of your Systems Director installation.

Tip: The Systems Director server must be stopped before you run the **smsave** command.

A description of the options for the **smsave** command is at this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_smsave.html

The backup image that is created by the **smsave** command is saved in the `install_root\backup\time_stamp` directory, unless you otherwise specified the output directory in the command.

The **smsave** command creates a backup image of Systems Director persistent data. Persistent data includes file system data (also called master data) and database data. The master data set contains information about the location of the database data set and uses that stored location when you run the restore operation. The database backup image is saved in the format that is specific to the database type. Backups cannot be moved from one database type and version to another database type or version.

When you run the command, the execution log is saved to `install_root\log\smave.log` and all status is updated in real time in that file. No output is posted to the command prompt.

Figure 4-1 shows an example of using the **smsave** command on a Microsoft Windows 2008 R2 System.

First, you see that if the Systems Director server is not stopped before you run the **smsave** command, an information error is displayed. Stop the Systems Director server before you run the command by running the **net stop dirserver** command on Windows. For Linux, use the **smstop** command instead.

After you stop the Systems Director server, you can run the **smsave** command. Figure 4-1 shows the messages that you see during the procedure.

```
PS C:\Program Files\IBM\Director\bin> smsave

The Director Server is currently active. Please stop the server before running this
command.

PS C:\Program Files\IBM\Director\bin> net stop dirserver
The IBM Systems Director Server service is stopping.....
The IBM Systems Director Server service was stopped successfully.

PS C:\Program Files\IBM\Director\bin> smsave
Command is running. Monitor live status and results in C:\Program
Files\IBM\Director\log\smsave.log

        1 file(s) copied.

ALR1325I: The lightweight runtime has started.
com.ibm.net.SocketKeepAliveParameters
        1 file(s) moved.

Command completed successfully

PS C:\Program Files\IBM\Director\bin>
```

Figure 4-1 *smsave* command

The log file, which is created during the backup process, is in the `install_root\log` directory. Figure 4-2 shows part of an example log file.

```
Command Execution for: Fri Oct 19 20:57:34 CEST 2012

Starting execution of Save Operation

Execution: Operation is save to the following location C:\Program
Files\IBM\Director\backup\2012_10_19_20.57.34

Execution: Loading aem.ext
Execution: Loading AgentFile.ext
Execution: Loading BaseFile.ext
Execution: Loading console.ext
Execution: Wildcard expression not matched to anything
-->lwi\runtime\isc\loginMessage\loginMessage*.properties
Execution: Loading database.ext
Execution: Loading databaseMigration.ext
Execution: Loading defaults.ext
Execution: Loading discovery.ext
Execution: Loading EventMapping.ext
Execution: Loading HMS.ext
Execution: Loading LegacyTablesExtension.ext
Execution: Loading LRTMMigration.ext
Execution: Loading MetricsMigration.ext
Execution: Loading security.ext
Execution: Loading skm.ext
Execution: Loading ssm.ext
Execution: Loading ssm_reset.ext
Execution: Loading StartAgentFile.ext
Execution: Loading StopAgentFile.ext
Execution: Loading StorageControlExt.ext
Execution: Loading ThresholdMigration.ext
Execution: Loading updates.ext
Execution: Loading vsm.ext
Execution: Loading Workflow.ext
Execution: Executing Extensions

Execution(20:57:34): Starting extension StopAgentFile.ext
Execution(20:58:48): Completed extension StopAgentFile.ext
Execution(20:58:48): Starting extension BaseFile.ext
BaseFileExt: save C:\Program Files\IBM\Director\version.srv to C:\Program
Files\IBM\Director\backup\2012_10_19_20.57.34\version.srv
BaseFileExt: save C:\Program Files\IBM\Director\data to C:\Program
Files\IBM\Director\backup\2012_10_19_20.57.34\data
....
```

Figure 4-2 *smsave.log* file

The data from the backup process is saved to the `install_root\backup` directory. The size depends several components:

- ▶ Number of systems that are discovered
- ▶ Inventory that is collected
- ▶ Update packages that are downloaded
- ▶ All other settings

In our simple lab tests, the initial backup that we performed after installation and an inventory run is about 60 MB in size.

4.2.2 Systems Director restore

Use the **smrestore** command to restore the persistent data, including file system (master) data and databases, from a backup image.

You can run the **smrestore** command locally from the management server. Or, run the command remotely by accessing the management server by using a remote access utility, such as Secure Shell (SSH) or Telnet.

To run the **smrestore** command, navigate to the `install_root\bin` directory, where `install_root` is the root directory of your Systems Director installation. The Systems Director server must be stopped before you run the **smrestore** command.

A description of the options for the **smrestore** command is at this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_smrestore.html

You can restore saved persistent data only on a management server with the same characteristics:

- ▶ Same operating system
- ▶ Same version of the Systems Director server from which the data was backed up
- ▶ Same database type and version

In addition, the Systems Director server and the database that you restore must be the same as the saved installation instances.

When you run the command, the execution log is recorded in the `install_root\log\smrestore.log` file, and all status is updated in real time in that file. Little information is posted to the command prompt.

Figure 4-3 shows the output from the command.

```
PS C:\Program Files\IBM\Director\bin> smrestore -sourceDir 'C:\Program
Files\IBM\Director\backup\201
2_10_19_20.57.34'
This operation will replace all current data with the specified backup set.
To continue, type "1" for yes or "0" for no.
1

Command is running. Monitor live status and results in C:\Program
Files\IBM\Director\log\smrestore.log

        1 file(s) copied.

ALR1325I: The lightweight runtime has started.
com.ibm.net.SocketKeepAliveParameters
        1 file(s) moved.

Command completed successfully

PS C:\Program Files\IBM\Director\bin>
```

Figure 4-3 *smrestore* command

4.2.3 Systems Director reset

The **smreset** command reinitializes the databases and clears all persistent data. The **smreset** command deletes local data on the file system where Systems Director is installed. The **smreset** command deletes and rebuilds all database tables that are used by Systems Director.

A description of the options for the **smrestore** command is at this website:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_smreset.html

Use the **smreset** command to return the Systems Director server to its installation default values. This command must also be run immediately after you run the **cfgdbcmd** command to change to a new database. For example, run the **smreset** command when you upgrade from a managed IBM DB2 database to an enterprise database such as Oracle Database. Run the **smreset** command only when the Systems Director server is stopped.

The **smreset** command does not delete or reset Agent Manager information. The **smreset** command deletes the following data:

- ▶ Discovered resource data (except for 6.x Common Agents that were previously accessed)
- ▶ Inventory data
- ▶ Event data (event log, custom event filters, custom event actions, and custom event plans)
- ▶ Monitoring data
- ▶ Updates data
- ▶ Status data
- ▶ Configuration templates
- ▶ Security configurations
- ▶ All other data that is associated with running and configuring Systems Director after the installation

The **smreset** command creates two log files, `smreset.log` and `reset.log`, which are in the `install_root\log` directory.

Figure 4-4 shows the output from the **smrestore** command.

```
PS C:\Program Files\IBM\Director\bin> smreset.bat
This operation will revert the IBM Systems Director database and server to the installed
state. To c
ontinue, type "1" for yes or "0" for no.
1
          1 file(s) copied.

ALR1325I: The lightweight runtime has started.
com.ibm.net.SocketKeepAliveParameters
          1 file(s) moved.

Command completed successfully

PS C:\Program Files\IBM\Director\bin>
```

Figure 4-4 *smreset* command

4.3 Migration

The tools that can be used to migrate from one version of a Systems Director to a newer version or to another system are described.

A backup and restore process can only be used if the management server, where a backup is restored, runs the same operating system. And the version of the Systems Director server must be the same as the version from which the data was saved. The database type and version must be the same. In addition, the Systems Director server and the database that you restore must be the same as the saved installation instances.

You can switch to another operating system, another system, or another database and take the settings from the former Systems Director server with you. Use the commands in Table 4-1 to export and import settings and managed endpoints.

Table 4-1 Command-line tools for migration

Command	Description
<code>dircli lsmo^a</code>	List managed objects - replaced by <code>smcli lssys</code>
<code>dircli mkmo^a</code>	Make managed objects
<code>smcli lsevtautopln</code>	List information about event automation plans. You can also export one or more event automation plans to a file.
<code>smcli mkevtautopln</code>	Create an event automation plan or import one or more existing event automation plans.

a. Before you use this command, issue the `set CLILEGACY=1` command.

For the complete list of the `smcli` commands and a description for each command, see the Systems Director Information Center:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.cli.helps.doc%2Ffqm0_r_cli_smcli.html

4.3.1 Exporting systems and settings

How to export the systems and settings (for example, event automation plans) from an existing Systems Director server by using command-line tools is described.

Exporting systems

Use the following command for exporting the existing systems to a file. This information can be used later on a new Systems Director server to import the systems without discovery:

```
./smcli lssys -t "OperatingSystem" -d ";" -A  
"Displayname,IPv4Address,Hostname,ManagementSoftware" >>OS.txt
```

In our lab example, the contents of the file that is created are shown in Figure 4-5.

```
9.42.171.194: 9.42.171.194;{ '9.42.171.194' };{ };{ '' }
9.42.171.195: 9.42.171.195;{ '9.42.171.195' };{ };{ '' }
9.42.171.196: 9.42.171.196;{ '9.42.171.196' };{ };{ '' }
9.42.171.197: 9.42.171.197;{ '9.42.171.197' };{ };{ '' }
9.42.171.198: 9.42.171.198;{ '9.42.171.198' };{ };{ '' }
9.42.171.199: 9.42.171.199;{ '9.42.171.199' };{ };{ '' }
9.42.171.203: 9.42.171.203;{ '9.42.171.203' };{ };{ '' }
9.42.171.22: 9.42.171.22;{ '9.42.171.22' };{ };{ '' }
9.42.171.23: 9.42.171.23;{ '9.42.171.23' };{ };{ 'IBM-IBM Director Agent-v6.3.2',
'IBM-IBM Director Platform Agent-v6.3.2' }
9.42.171.232: 9.42.171.232;{ '9.42.171.249', '9.42.171.232' };{ };{ '' }
9.42.171.244: 9.42.171.244;{ '9.42.171.244' };{ };{ '' }
9.42.171.25: 9.42.171.25;{ '9.42.171.25' };{ };{ '' }
9.42.171.254: 9.42.171.254;{ '9.42.171.254' };{ };{ '' }
9.42.171.26: 9.42.171.26;{ '9.42.171.32', '9.42.171.26', '9.42.171.29', '9.42.171.30',
'9.42.171.31', '9.42.171.33', '9.42.171.34' };{ };{ '' }
9.42.171.27: 9.42.171.27;{ '9.42.171.27' };{ };{ '' }
9.42.171.28: 9.42.171.28;{ '9.42.171.28' };{ };{ '' }
9.42.171.40: 9.42.171.40;{ '9.42.171.40' };{ };{ '' }
9.42.171.54: 9.42.171.54;{ '9.42.171.55', '9.42.171.54', '9.42.171.56' };{ };{ '' }
9.42.171.60: 9.42.171.60;{ '9.42.171.60' };{ };{ '' }
9.42.171.62: 9.42.171.62;{ '9.42.171.62' };{ };{ '' }
9.42.171.82: 9.42.171.82;{ '9.42.171.82' };{ };{ '' }
9.42.171.86: 9.42.171.86;{ '9.42.171.86' };{ };{ 'IBM-IBM Director Agent-v6.3.2',
'IBM-IBM Director Platform Agent-v6.3.2' }
9.42.171.97: 9.42.171.97;{ '9.42.171.97' };{ };{ 'IBM-IBM Director Core
Services-v6.2.1.2', 'IBM-IBM Director Agent-v6.2.1' }
9.42.171.99: 9.42.171.99;{ '9.42.171.99' };{ };{ 'IBM-IBM Director Agent-v6.3.2',
'IBM-IBM Director Core Services-v6.3.2' }
SLES11: SLES11;{ '9.42.171.84' };{ 'SLES11' };{ 'IBM-IBM Director Agent-v6.3.2',
'IBM-IBM Director Platform Agent-v6.3.2' }
```

Figure 4-5 Output of the `smcli lssys` command

4.3.2 Exporting settings

Use the Systems Director command-line tools to export settings, such as event automation plans and groups. You can export settings in two ways:

- ▶ Use the `smcli i` command line, for example, to export event automation plans (Figure 4-6 on page 227).
- ▶ Use export functions in the Systems Director web interface (exporting groups as shown in Figure 4-7 on page 227).

To export the event automation plan, use the `smcli lsevtautopln` command. In our lab example, Figure 4-6, we exported the “Send eMail to Admin” event automation plan to the `EAPexport.xml` file. Use the `-o` attribute for an easier export because you can use the object identifier (OID) instead of the complete name.

```
SLES11:/opt/ibm/director/bin # ./smcli lsevtautopln
Log All Events
Send eMail to Admin
SLES11:/opt/ibm/director/bin # ./smcli lsevtautopln -o
Log All Events, 0x11
Send email to Admin, 0x11
SLES11:/opt/ibm/director/bin # ./smcli lsevtautopln -F xml 0x11 /tmp/EAPexport.xml
```

Figure 4-6 Export event automation plan

To export groups, you can use the Systems Director web interface. Start from the Resource Explorer Groups view and select the group that you want to export (Figure 4-7).

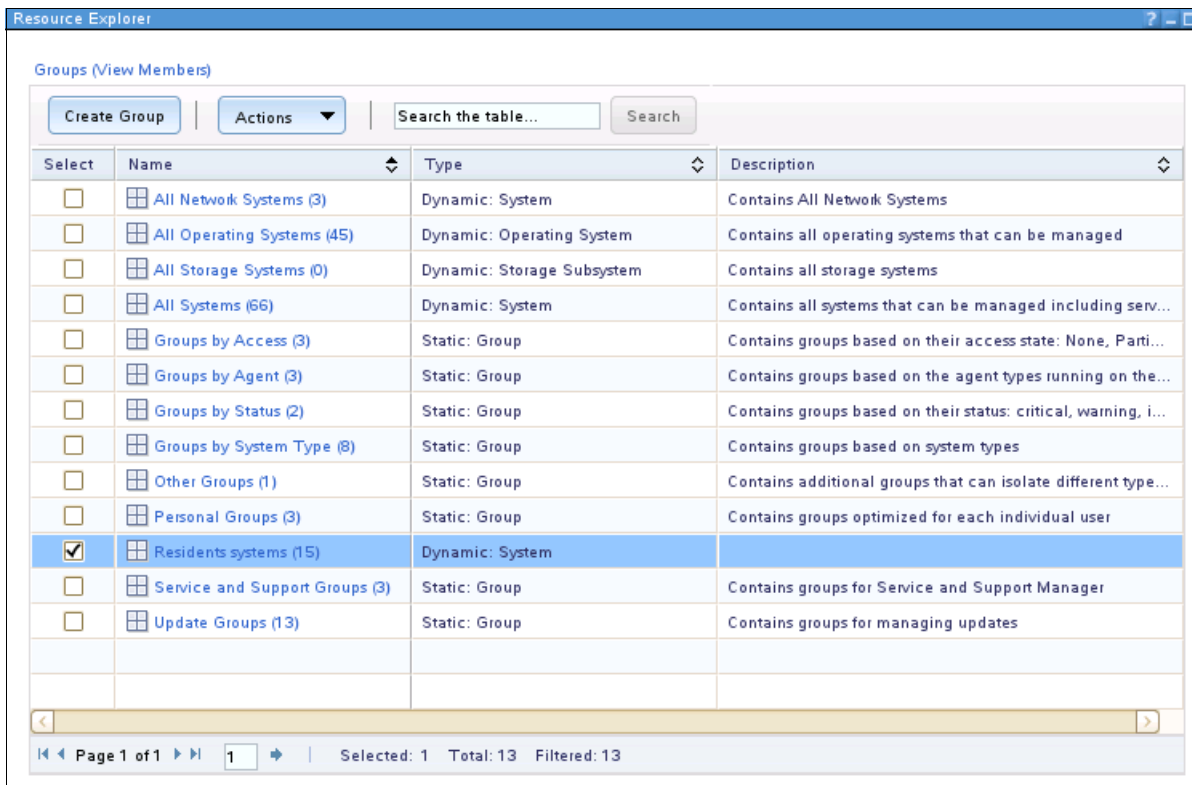


Figure 4-7 Groups in Resource Explorer

With the group selected, click **Actions** → **Export Group**.

Figure 4-8 opens where you can select to which directory you want to save the data. The file is named group `_%username%.xml`. The `username` is the user that is logged on and creates the export file.

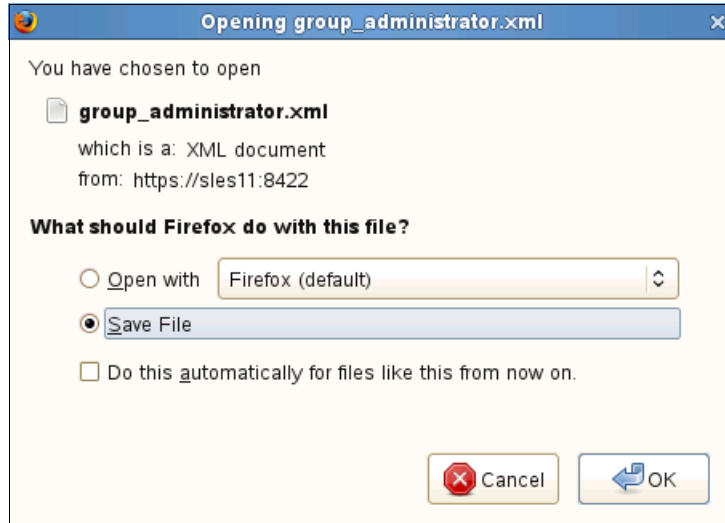


Figure 4-8 Save group data

You can use the file to import the group and the members of the group to another Systems Director server or use the file for recovery options.

4.3.3 Importing systems and settings

With Systems Director, you can use command-line tools to import systems and to request access to those systems. The command to import systems is `smcli mkmo (dircli mkmo)`.

Prerequisite: Before you run the `smcli mkmo (dircli mkmo)` command, issue the following command:

```
set CLILEGACY=1
```

Use the `smcli mkmo` command to create a managed object for the server and systems. The server represents the hardware service processor and the systems represent the operating system and agent.

In Figure 4-9, we first check whether the system is available. Then, we remove the system and check again whether the system exists. Then, we show the settings for `mkmo` and add the system to the Systems Director server again with the `smcli mkmo` command. We check again whether the system exists.

```
SLES11:/opt/ibm/director/bin # ./smcli lssys 9.42.171.196
9.42.171.196
SLES11:/opt/ibm/director/bin # ./smcli rmno 9.42.171.196
SLES11:/opt/ibm/director/bin #
SLES11:/opt/ibm/director/bin # ./smcli lssys 9.42.171.196
DNCZCLI0239E : (Run-time error) The system named 9.42.171.196 was not found
use the smcli lssys command to view all the valid system names
SLES11:/opt/ibm/director/bin #
SLES11:/opt/ibm/director/bin # ./smcli mkmo
Server:
type=Server
name=<Specify Name> (Optional)
ip=<Specify IP Address>

Systems:
type=Systems
name=<Specify Name> (Optional)
ip=<Specify Network Address>
network=<Specify Network Protocol> (Optional)
Available Protocols: TCPIP

SLES11:/opt/ibm/director/bin # ./smcli mkmo type=Systems ip=9.42.171.196
SLES11:/opt/ibm/director/bin #
SLES11:/opt/ibm/director/bin # ./smcli lssys 9.42.171.196
9.42.171.196
```

Figure 4-9 `smcli mkmo` command

You can also run the `smcli mkmo` command in a script. With a script, you can add many systems to the new Systems Director at the same time.

If you saved groups, you can import them to a new system. From the Resource Explorer, follow these steps:

1. Click **Action** → **Import Group** as shown in Figure 4-10.

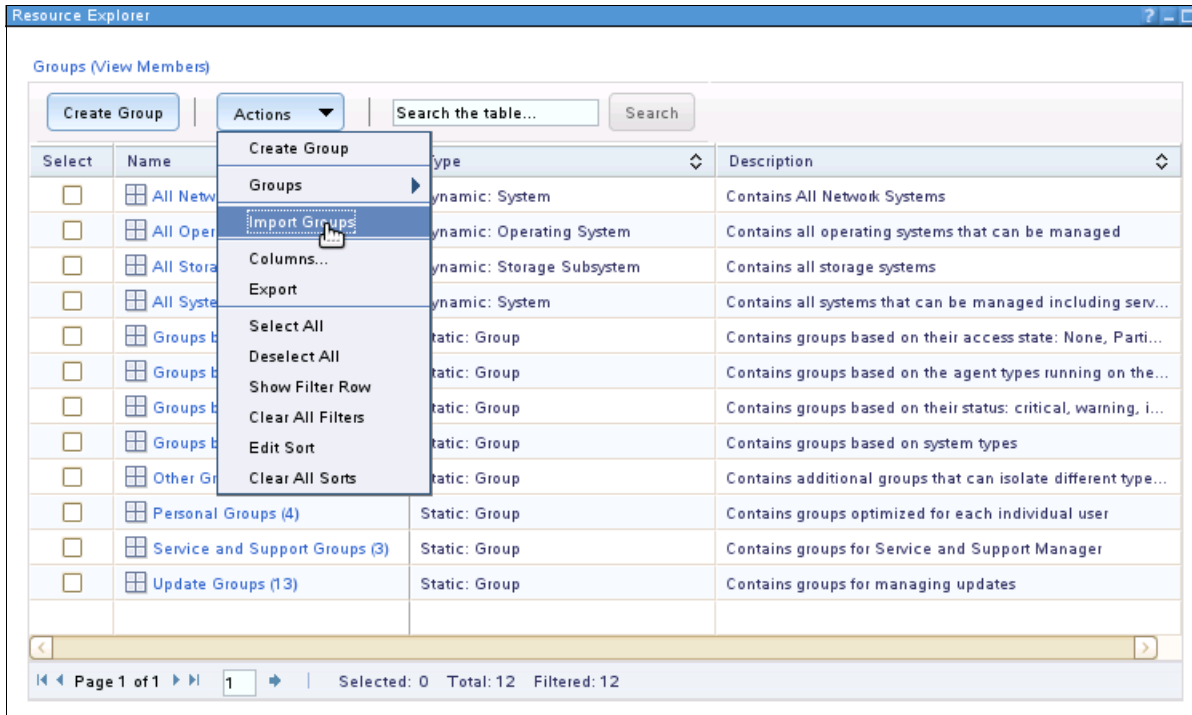


Figure 4-10 Import Groups

2. Figure 4-11 opens where you can browse for the XML file that contains the group information.



Figure 4-11 Select the file with the group information

3. The imported groups show under **Groups** → **Personal Groups** as shown in Figure 4-12 on page 231.

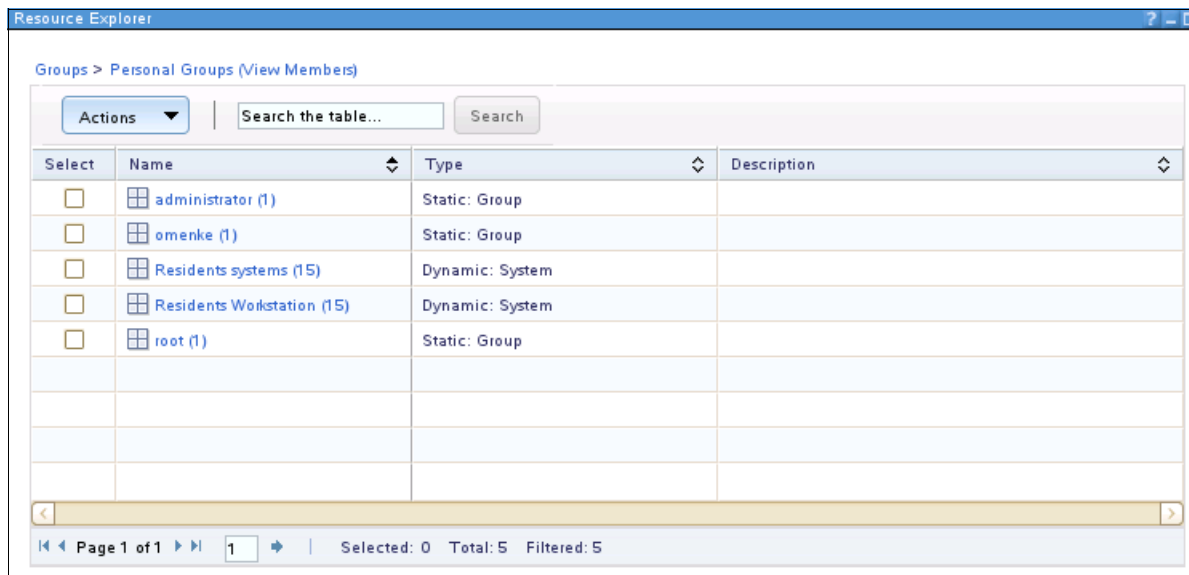


Figure 4-12 Groups: Personal groups view

To import a saved event automation plan, run the `smcli mkevtautopln /tmp/EAPexport.xml` command as listed in Figure 4-13. In our example, we use the event automation plan that we exported before to the `EAPexport.xml` file.

```
SLES11:/opt/ibm/director/bin # ./smcli mkevtautopln /tmp/EAPexport.xml
Warning Number: 1
DNZEAP2068W: (Run-time warning)
The IP address or host name 'smtp.itso.ral.ibm.com' is not accessible.

Action name: eMail to Admin
Element name: EmailSmtServer
Element value: smtp.itso.ral.ibm.com

Warning Number: 2
DNZEAP2059W: (Run-time warning)
The event filter named 'Critical Events' has the same name and definition as an existing
filter in the system.
The filter will be not be created again.

Filter name: Critical Events

Total number of warnings: 2

DNZEAP2064I: (Informational) Created event action 'eMail to Admin'.
DNZEAP2066I: (Informational) Created event automation plan 'Send eMail to Admin'.
DNZEAP2067I: (Informational) Targets 'All Systems', applied to event automation plan
'Send eMail to Admin'.
SLES11:/opt/ibm/director/bin #
```

Figure 4-13 Importing an event automation plan

During the import process, the event automation plan is checked. Warnings display if incorrect settings exist in the event automation plan or if event actions or filters exist on the system. The existing filter or event action is not created again. You can see that the event Action plan “Send eMail to Admin” is created. All systems, predefined in the event automation plan that we exported, are assigned to this event automation plan.



Additional information and education

How and where to get information and education about IBM Systems Director are described.

The following topics are included:

- ▶ 5.1, “Information center” on page 234
- ▶ 5.3, “Education and training” on page 237
- ▶ 5.4, “Downloads” on page 241
- ▶ 5.5, “Other useful links” on page 242

5.1 Information center

One of the first sources for information is the Systems Director Information Center. The Systems Director Information Center is an online and regularly updated version of the Systems Director product publications. For the latest version of Systems Director, see this website:

<http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp>

If you use older versions of Systems Director, you can see the URLs to the information center in Table 5-1.

Table 5-1 Information center links

IBM Systems Director version	Information center
6.2.x	Systems Director version 6.2.x Information Center: http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp
6.1.x	Systems Director version 6.1.x Information Center: http://publib.boulder.ibm.com/infocenter/director/v6r1x/index.jsp
5.2.x	IBM Director version 5.20.x Information Center: http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diricinfo_5.20/fqm0_main.html

In the information center, you can search for information about the installation, configuration, management, and problem determination. You can also download the PDF versions of the installation guide, planning guide, troubleshooting guide, and systems management guide.

5.2 Social media and support

Other users are a great source of help with Systems Director.

5.2.1 Forum

The Systems Director forum is available through the following link:

<http://www.ibm.com/developerworks/forums/forum.jspa?forumID=759>

This forum provides a place for all Systems Director discussion topics. You can post your questions and comments, and share your thoughts, ideas, and solutions with other users.

The forum also offers an RSS feed. To subscribe to this feed, go to this website:

<http://www.ibm.com/developerworks/forums/forum.jspa?forumID=759>

Look for the orange RSS icon near the upper-middle part of the page. On the RSS subscription page, select the method to use to subscribe to the feed and click **Subscribe Now** (Figure 5-1).

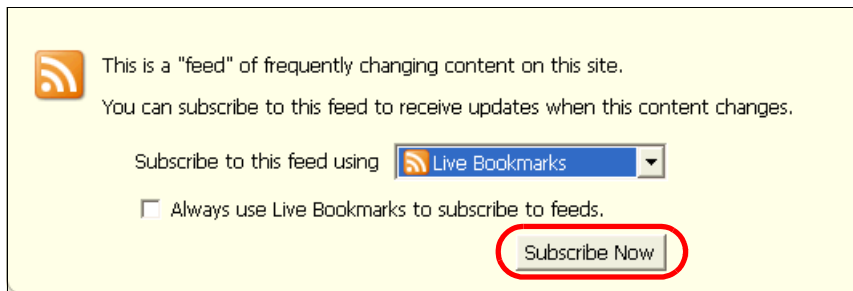


Figure 5-1 Systems Director Forum RSS feeds

5.2.2 Wiki

There are two wikis for Systems Director. Both wikis are focused on Systems Director running on a Power platform. However, some of the information applies to all platforms:

- ▶ Systems Director Wiki:

<https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Power%20Systems/page/IBM%20Systems%20Director>

- ▶ Systems Director Best Practices Wiki:

<http://www.ibm.com/developerworks/wikis/display/WikiPtype/IBM+Systems+Director+Best+Practices+Wiki>

5.2.3 YouTube channel

To subscribe to this channel, go to <http://www.youtube.com/user/IBMSystemsDirector/feed> (Figure 5-2) and click **Subscribe**.

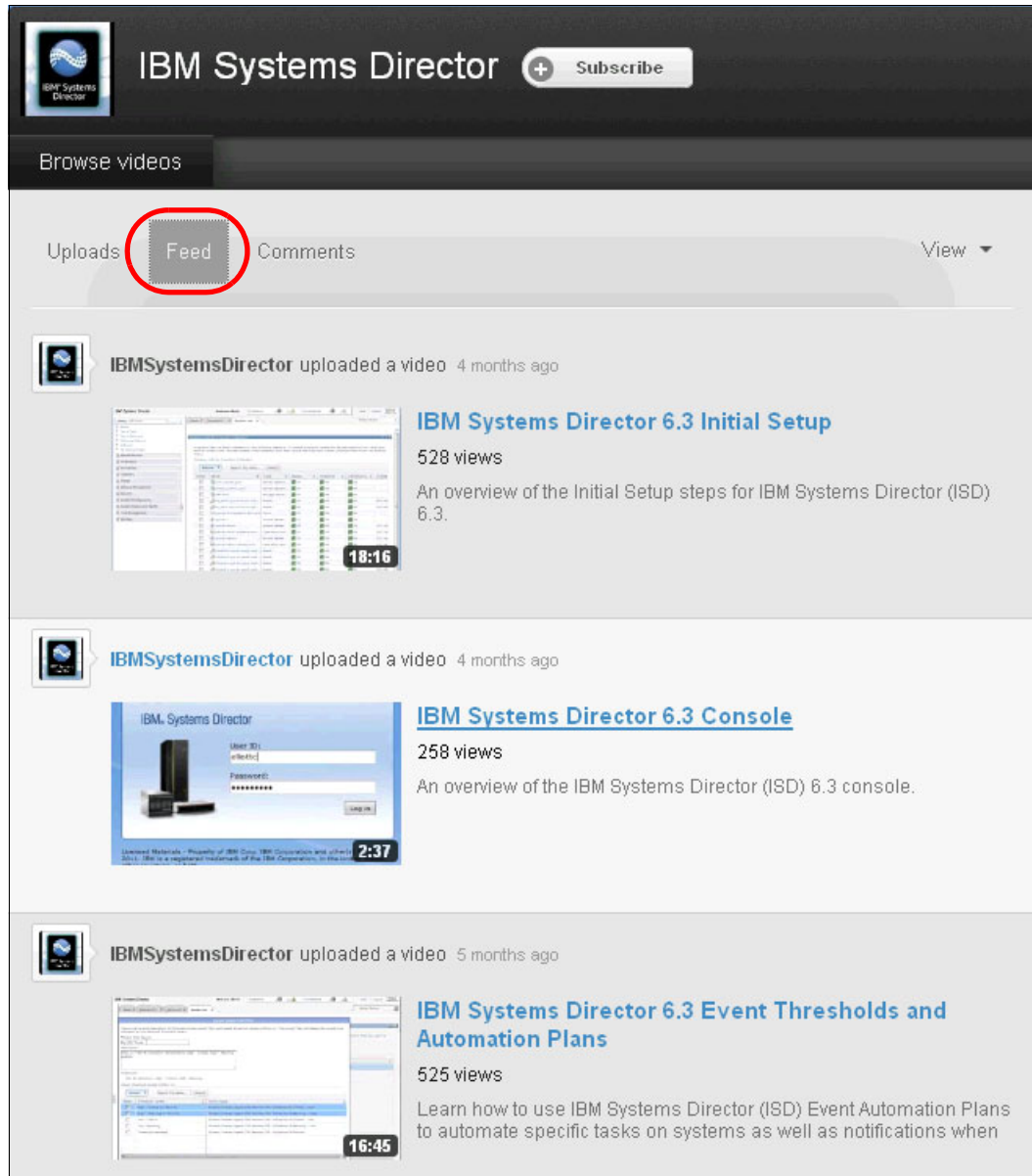


Figure 5-2 Systems Director at YouTube

5.2.4 Facebook page

Systems Director is on Facebook:

<https://www.facebook.com/pages/IBM-Systems-Director/193362963483>

Click **Like** to receive updates on your own Facebook timeline or news feed.

5.2.5 My Notifications email announcements

With My Notifications, you can subscribe to Support updates for any IBM product.

Tip: My Notifications replaces My Support, a similar tool.

With My Notifications, you can specify that you want to receive daily or weekly email announcements. You can specify the type of information that you want to receive:

- ▶ Publications
- ▶ Hints and tips
- ▶ Product flashes (also known as *alerts*)
- ▶ Downloads
- ▶ Drivers

With My Notifications, you can customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Complete the following steps to subscribe to My Notifications:

1. Go to <http://www.ibm.com/support/mynotifications>.
2. Enter your IBM ID and password¹ and click **Submit**.
3. Identify the updates that you want to receive and the method through which you want to receive them:
 - a. Click the **Subscribe** tab.
 - b. Select **IBM Systems Director**.
 - c. Specify or select your notifications and other preferences.
 - d. Click **Submit**.

5.3 Education and training

IBM offers various educational offerings, including instructor-led online (ILO) courses, classroom courses, virtual learning courses, private/on-site training, and web-based learning videos. Links are available in the Systems Director console for online training.

¹ If you have no IBM ID and password, you can request this information on the logon site. The ID and password are no-charge.

5.3.1 Integrated education modules in Systems Director

The Systems Director console provides links for online training. The links are on the Systems Director home page under the Learn tab as shown in Figure 5-3.

The screenshot shows the IBM Systems Director console interface. The browser address bar displays `https://localhost:8422/ibm/console/login.do?action=secure`. The main navigation bar includes "Welcome Diradmin", "Problems", "Compliance", and "Help". A left-hand sidebar lists various system management categories such as Automation, Inventory, Release Management, Security, System Configuration, System Status and Health, Task Management, Remote Access, and Settings. The main content area features a "Home" tab and a "Learn" tab, which is circled in red. Below the tabs, there is a section for initial setup tasks with the heading "Perform the following initial setup tasks to set up IBM® Systems Director for the first time." The tasks listed are: 1. Update IBM® Systems Director (with a sub-link for "Learn more about restarting the IBM® Systems Director server"), 2. System Discovery (with a status report: "Systems have been discovered: 1 Operating system, 0 systems with no agent, 0 systems with Platform Agent, 1 system with Common Agent"), 3. Request Access (with a status report: "0 systems have no access"), and 4. Collect inventory (with a status report: "1 system has no inventory collected"). A "Common Links" section at the bottom provides quick access to "Resource Explorer" and "Health Summary".

Figure 5-3 IBM Director Console home page

On the Learn page, you can see the available learning modules for Systems Director (Figure 5-4).

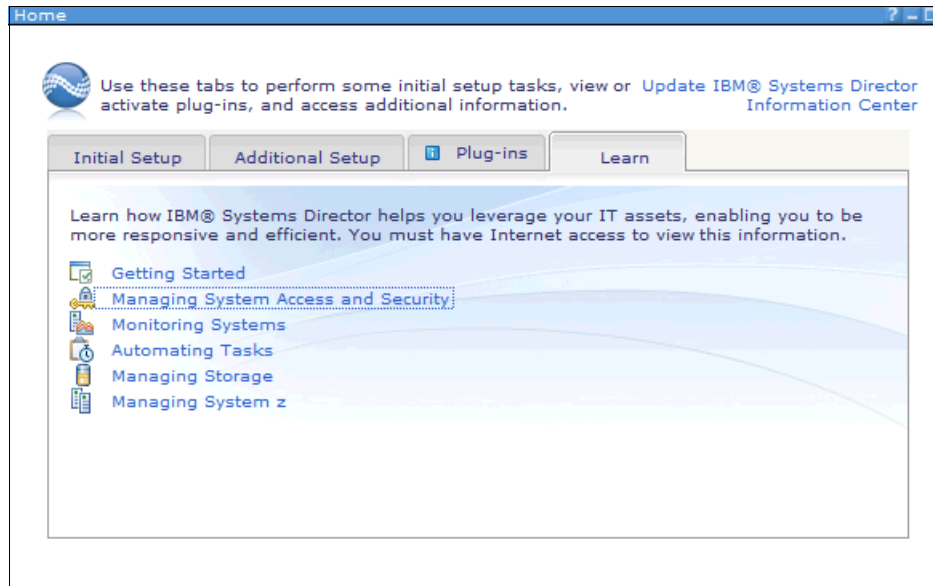


Figure 5-4 Learn tab

When you click one of the topics, you link to the Systems Director Information Center website. Videos for the selected topic are displayed. In our example, we select the “Managing system access and security” topic (Figure 5-5).

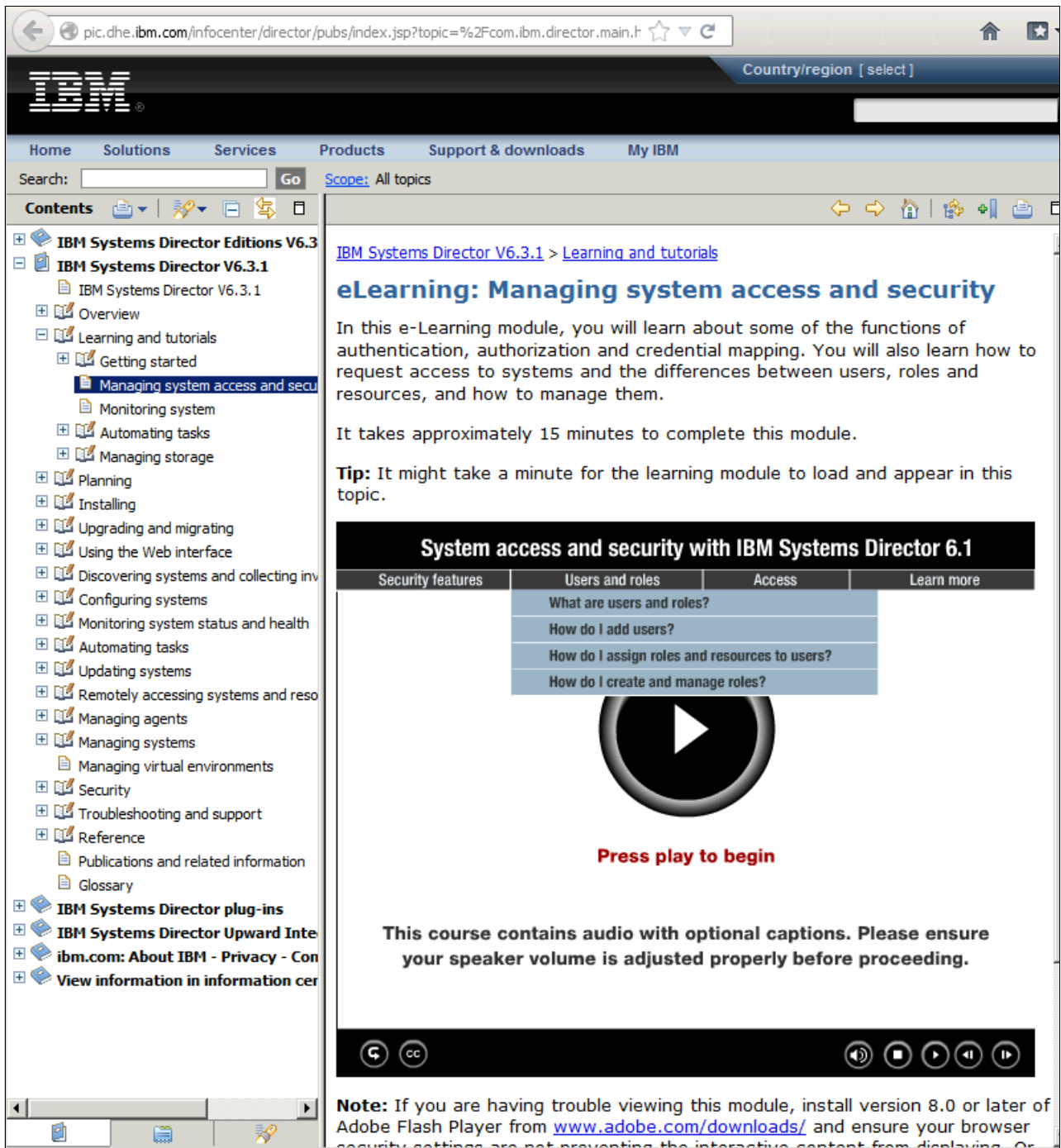


Figure 5-5 Managing system access and security module

You can also access the training modules at the Systems Director Information Center through the following link:

http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp?topic=%2Fcom.ibm.director.main.helps.doc%2Ffqm0_c_elearning.html

5.3.2 Education courses

The following Classroom (XTR) courses and ILO (XTV) courses for Systems Director 6.3 are available in the US at the time of writing:

- ▶ XTR/XTV 42 - IBM Systems Director 6.3 Hands-on Workshop
- ▶ XTR/XTV 46 - IBM Systems Director 6.3 - Introduction
- ▶ XTR/XTV 47 - IBM Systems Director 6.3 for IBM System x and BladeCenter Servers - Base
- ▶ XTR/XTV 48 - IBM Systems Director 6.3 for IBM System x and BladeCenter Servers - Advanced
- ▶ XTRD1+2/XTVD1+2 - IBM Systems Director 6.3 for IBM System x and BladeCenter Servers
- ▶ AN940/AX940 - IBM Systems Director 6.3 for Power Systems I: Installation and Management

A self-paced virtual class (SPVC) is available:

- ▶ AN0D0/XTRD0 - IBM Systems Director 6.3 - Power and System x - Planning and Installation

The availability of on-site or classroom training depends on your country. For detailed information about the offerings in your country, see the following link:

<http://www-304.ibm.com/jct03001c/services/learning/ites.wss/zz/en?pageType=page&c=a0011023>

Complete the following steps to check the availability of Learning courses in your country:

1. Go to the link:

<http://www-304.ibm.com/jct03001c/services/learning/ites.wss/zz/en?pageType=page&c=a0011023>

2. Select your country and click the arrow.

3. Scroll to the bottom of the page and click **Training Search**.

4. Type IBM Systems Director 6.3 in the search field and click **Search**.

5. The available courses are displayed.

6. Select your course.

5.4 Downloads

All downloads for Systems Director, including server, Agents, and Plug-ins, are at the following link:

<http://ibm.com/systems/software/director/downloads>

On the Downloads overview page, you see information about the recent product updates that you can download (Figure 5-6). By selecting the tabs for Management servers, Agents, Plug-ins, and Partner integration, you can access the pages for download.

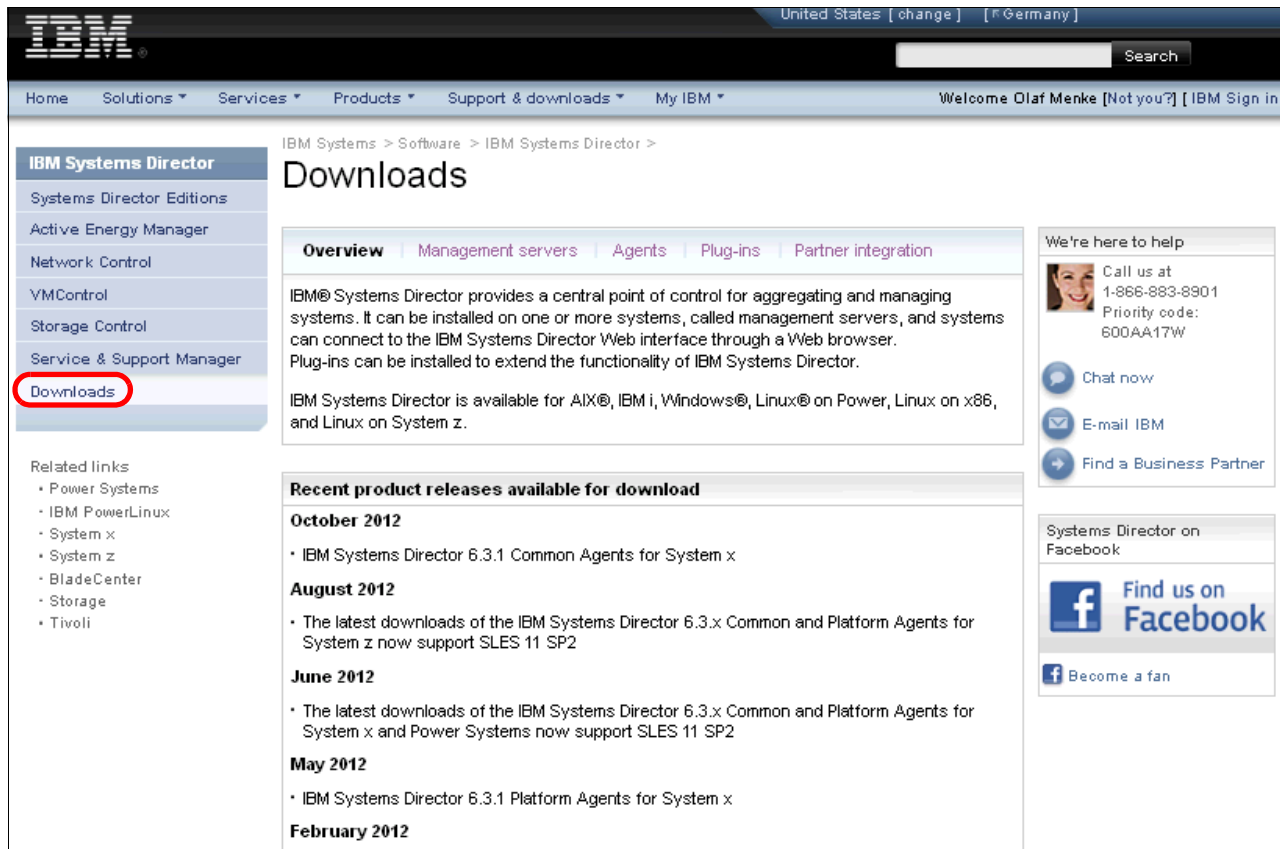


Figure 5-6 Downloads for Systems Director

5.5 Other useful links

The following references are useful:

- ▶ xREF: IBM x86 Server Reference:
<http://www.redbooks.ibm.com/xref>
- ▶ IBM Configuration and Options Guide (COG):
<http://ibm.com/support/entry/portal/docdisplay?ln docid=SCOD-3ZVQ5W>
- ▶ BladeCenter Interoperability Guide:
<http://ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5073016>
- ▶ IBM Flex System Interoperability Guide:
<http://www.redbooks.ibm.com/fsig>
- ▶ IBM ToolCenter (ServerGuide, Bootable Media Creator, Advanced Settings Utility):
<http://ibm.com/support/entry/portal/docdisplay?ln docid=TOOL-CENTER>
- ▶ IBM BladeCenter Information Center:
<http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp>

- ▶ IBM PureFlex System Information Center:
<http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp>
- ▶ IBM Power Systems Hardware Information Center (including IBM System p®, IBM System i, and Hardware Management Console information):
<http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=/ipha8/hwicwelcome.htm>

Abbreviations and acronyms

AES	Advanced Encryption Standard	SDD	Subsystem Device Driver
AMM	Advanced Management Module	SLP	Service Location Protocol
BMC	Baseboard Management Controller	SMTP	Simple mail transfer protocol
CAS	Column address strobe	SNMP	Simple Network Management Protocol
CIM	Common Information Model	SQL	Structured Query Language
CLI	Command-line interface	SSH	Secure Shell
CMM	Chassis Management Module	SSL	Secure Sockets Layer
COG	Configuration and option guide	SSO	Single sign-on
CSV	Comma-separated variable	TPM	Trusted Platform Module
DCOM	Distributed Component Object Model	UDP	User datagram protocol
DMZ	Demilitarized zone	UEFI	Unified Extensible Firmware Interface
DNS	Domain Name System	UI	User interface
EAP	Event Action Plan	UID	Unique ID
ESA	Electronic Service Agent	UXSPI	UpdateXpress System Packs Installer
FCM	Fast communication manager	VIOS	Virtual I/O Server
FSM	Flex System Manager	WLE	Workload Estimator
GID	Group ID	XML	Extensible Markup Language
GUI	Graphical user interface		
HMC	Hardware Management Console		
IMM	Integrated Management Module		
IPC	Interprocess communication		
ISD	Integrated System Development		
ISO	International Organization for Standards		
IVM	Integrated Virtualization Manager		
LDAP	Lightweight Directory Access Protocol		
LDIF	LDAP Data Interchange Format		
LED	Light emitting diode		
LPAR	Logical partitions		
LPD	Light path diagnostic		
NIM	Network Installation Management		
OID	Object identifiers		
PID	Product ID		
PMR	Problem management record		
PTF	Program temporary fix		
RBAC	Role-based access control		
RPM	Red Hat Package Manager		
RSA	Remote Supervisor Adapter		
RSS	Really Simple Syndication		

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- ▶ *IBM BladeCenter Products and Technology*, SG24-7523
- ▶ *IBM PureFlex System and IBM Flex System Products and Technology*, SG24-7984

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- ▶ IBM Systems Director home page
<http://ibm.com/systems/software/director/>
- ▶ IBM Systems Director downloads
<http://ibm.com/systems/software/director/downloads>
- ▶ IBM Systems Director 6.3 Information Center
<http://pic.dhe.ibm.com/infocenter/director/pubs/index.jsp>
- ▶ IBM Systems Director 6.2.x Information Center
<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp>
- ▶ IBM Systems Director 6.1.x Information Center
<http://publib.boulder.ibm.com/infocenter/director/v6r1x/index.jsp>
- ▶ IBM Director 5.20.x Information Center
http://pic.dhe.ibm.com/infocenter/director/v5r2/index.jsp?topic=/diricinfo_5.20/fqm0_main.html
- ▶ The IBM Systems Director support forum
<http://www.ibm.com/developerworks/forums/forum.jspa?forumID=759>
- ▶ YouTube Channel
<http://www.youtube.com/user/IBMSystemsDirector>

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



IBM Systems Director 6.3 Best Practices Installation and Configuration



Provides additional guidance beyond the information center

Covers Windows, Linux, and AIX operating systems

Written by experts in the field

IBM Systems Director is a platform management foundation that streamlines the way that physical and virtual systems are managed. Using industry standards, IBM Systems Director supports multiple operating systems and virtualization technologies.

This paper provides guidance and preferred practices about how to install and configure IBM Systems Director Version 6.3. Also, installation guidance, fundamental topics, such as discovery and inventory, and more advanced topics, such as troubleshooting and automation, are covered.

This paper is meant to be a partner to the comprehensive documentation in the IBM Systems Director Information Center. This paper is aimed at IT specialists who are planning to install and configure IBM Systems Director on Microsoft Windows, Linux, or IBM AIX.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks