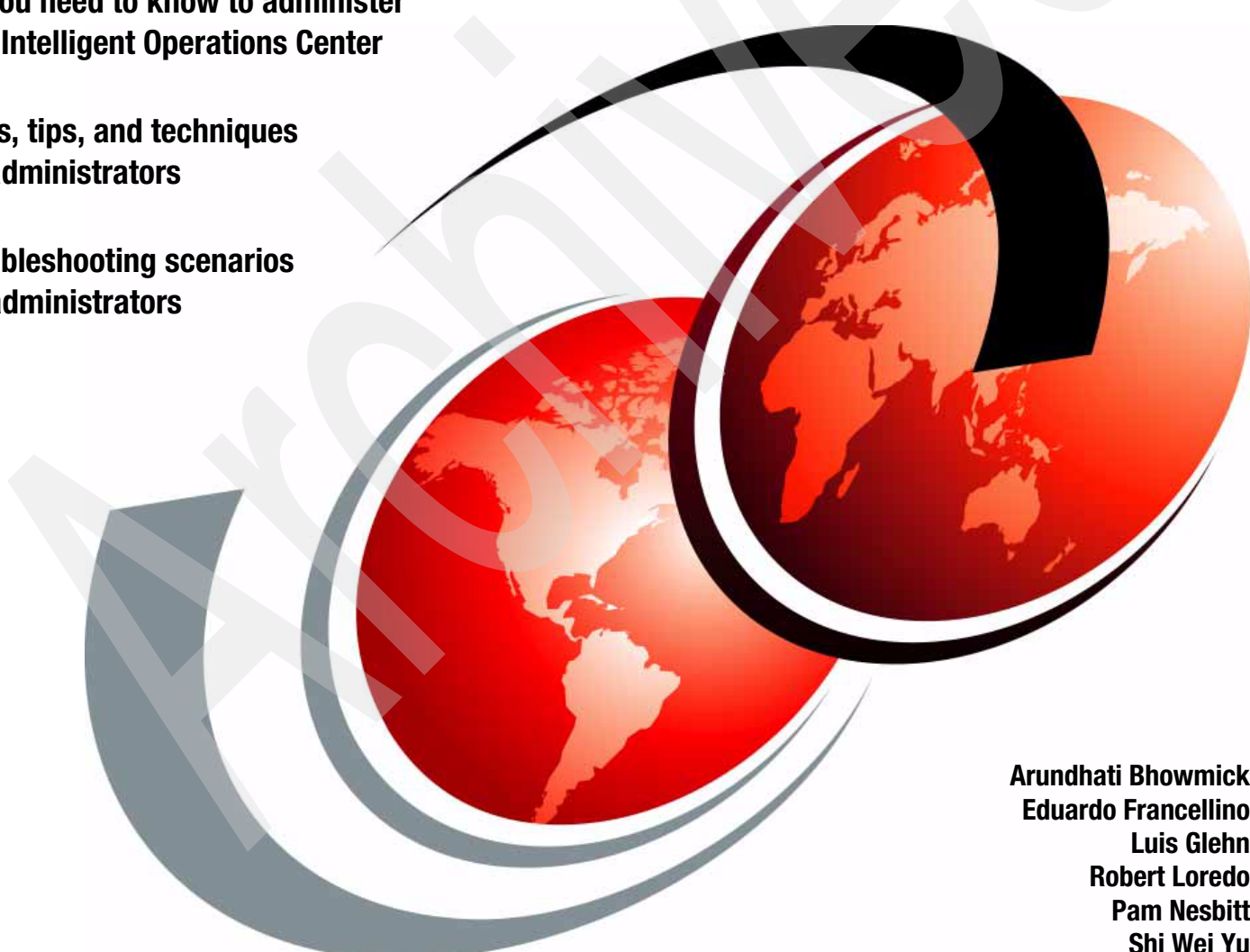


IBM Intelligent Operations Center for Smarter Cities Administration Guide

All you need to know to administer
IBM Intelligent Operations Center

Tools, tips, and techniques
for administrators

Troubleshooting scenarios
for administrators



Arundhati Bhowmick
Eduardo Francellino
Luis Glehn
Robert Loredo
Pam Nesbitt
Shi Wei Yu

Redbooks



International Technical Support Organization

**IBM Intelligent Operations Center for Smarter Cities
Administration Guide**

November 2012

Archived

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

Archived

First Edition (November 2012)

This edition applies to Version 1.5 of the IBM Intelligent Operations Center for Smarter Cities.

© Copyright International Business Machines Corporation 2012. All rights reserved.

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

Contents

Figures	vii
Tables	xi
Examples	xiii
Notices	xv
Trademarks	xvi
Preface	xvii
The team who wrote this book	xvii
Now you can become a published author, too!	xix
Comments welcome.	xix
Stay connected to IBM Redbooks	xx
Chapter 1. IBM Intelligent Operations Center overview	1
1.1 What a Smarter City is	2
1.1.1 Challenges facing city leaders today.	2
1.2 What IBM Intelligent Operations Center is	3
1.2.1 Business value	4
1.2.2 Key concepts	5
1.3 Solution overview	8
1.3.1 Visual workspace	9
1.3.2 Events and incident management.	9
1.3.3 Resource, response, and activity management	11
1.3.4 Status monitoring	11
1.3.5 Collaboration, instant notification, and messaging	12
1.3.6 Reports	12
1.3.7 Semantic model	13
1.4 Typical flow	14
1.5 Solution architecture	15
1.6 Usage scenarios	16
1.6.1 Advanced emergency response system	16
1.6.2 Wastewater management	17
1.6.3 Entertainment venue operations center	18
1.7 New features of IBM Intelligent Operations Center V1.5	19
1.7.1 Supported platforms	21
1.7.2 Ordering information	21
1.7.3 Related information	21
1.8 Scope and content of this publication	22
Chapter 2. Topology	23
2.1 High-level architecture	24
2.1.1 Servers overview	24
2.1.2 Services overview	26
2.2 System topology	29
2.2.1 Topology overview	30
2.2.2 Elements common to all servers	31
2.2.3 Topology of the application server	32

2.2.4	Topology of the event server	34
2.2.5	Topology of the data server	37
2.2.6	Topology of the management server	39
2.3	Hardware and software environment that is used in this publication	41
Chapter 3. Administration fundamentals		43
3.1	Platform control tool (IOControl or PCT).	44
3.1.1	Starting servers with IOControl.	46
3.1.2	Stopping servers with IOControl.	46
3.1.3	Querying the server status with IOControl	47
3.2	System Verification Check	48
3.2.1	Running System Verification Check tests	49
3.2.2	Performing problem determination procedures.	52
3.3	Administration Consoles	55
3.4	Sample Event Publisher portlet.	59
3.4.1	Creating test events	60
3.4.2	Creating test KPI messages	62
3.4.3	Creating test notifications	64
3.5	System monitoring	65
3.6	WebSphere MQ Explorer	72
3.7	Database control center	74
3.8	IBM Tivoli Netcool/OMNibus database utility	76
3.9	MustGather tool.	78
3.10	System-wide configuration properties	80
3.11	Solution logs	80
3.12	Checking the health of the solution	82
Chapter 4. Preventive maintenance		83
4.1	Backing up and archiving log files.	84
4.1.1	Backing up log files	84
4.1.2	Archiving log files	86
4.2	Database maintenance	86
4.2.1	Database table pruning.	88
4.3	Backing up and restoring	90
4.3.1	Backing up databases.	90
4.3.2	Virtual infrastructure snapshots.	96
4.4	Testing and production environments	96
4.5	Tivoli Enterprise Portal	97
Chapter 5. Security considerations		101
5.1	User IDs and password management.	102
5.1.1	Service user IDs shipped with IBM Intelligent Operations Center.	102
5.1.2	Password management for service users.	104
5.1.3	Sample solution users shipped with IBM Intelligent Operations Center	105
5.1.4	User policy settings for solution users.	105
5.1.5	User password policies.	109
5.1.6	Importing users from a user registry	109
5.2	Access control.	109
5.2.1	Web resource permissions	110
5.2.2	Portal resource permissions and user role groups	111
5.2.3	Data permissions and user category groups.	117
5.2.4	User permissions summary.	119
5.2.5	IBM Tivoli Directory Server Web Administration Tool	121
5.3	User management quick start scenarios.	123

5.3.1	Adding a user with the operator role and permissions in order to view transportation data.	123
5.3.2	Checking user permissions.	127
5.3.3	Validating user permissions	127
5.3.4	Changing a user's password.	128
5.3.5	Deleting a user	129
5.4	Directory server backup and restore	130
5.4.1	Exporting LDAP users example	130
5.4.2	Exporting LDAP groups example	131
5.5	Single sign-on	132
5.5.1	Implementing SSO with a new back-end service	133
5.6	Troubleshooting security problems	135
5.6.1	Security logs	135
5.6.2	Tracing security components	135
Chapter 6.	Troubleshooting	137
6.1	Troubleshooting scenarios	138
6.1.1	Events that are not displayed in the Details portlet.	138
6.1.2	Activities not displayed in the <i>My Activities</i> portlet	149
6.1.3	KPIs not displayed in the Status or Drill Down portlets.	155
6.1.4	Notifications not displayed in portlet	164
6.1.5	Correlated notification not displayed.	169
6.1.6	Resources are not being updated.	173
6.1.7	Event Publisher tool not publishing events on the Details portlet	178
6.1.8	Unable to log in to the IBM Intelligent Operations Center.	179
6.1.9	Login shows "Third-party server not responding" error message	180
6.1.10	Cannot access the login window.	180
6.1.11	Portlets error "An error has occurred communicating with the servers"	181
6.1.12	User login expired error.	181
6.1.13	Login shows the "Error 403: Authentication Failed" error	182
6.1.14	Portal shows the error message "There is no content available"	184
6.1.15	Portlets on the IBM Intelligent Operations Center page are closed	185
6.1.16	Contacts portlet prompts for user name and password	185
6.1.17	The Cognos Report page shows a server error	186
6.1.18	The KPI portlet is not refreshing the status.	187
6.1.19	IBM Intelligent Operations Center page loads slowly	187
6.2	Troubleshooting resources and references.	187
6.2.1	IBM Support portal	187
6.2.2	IBM Service Request tool	187
6.2.3	IBM Support Assistant	188
Chapter 7.	Data flows	189
7.1	Event flow	190
7.2	Key performance indicators flow	196
7.3	Correlation flow	203
7.4	Notification flow	206
7.5	Resource flow	211
7.6	User authentication and authorization flow	218
7.7	Overall system flows	220
Related publications	223	
IBM Redbooks	223	
Other publications	223	
Online resources	224	

Archived

Figures

1-1	Components of a Smarter City	2
1-2	IBM Intelligent Operations Center operator dashboard	5
1-3	IBM Intelligent Operations Center visual workspace	9
1-4	Geospatial and detailed representation of events	10
1-5	Event details and operator actions	11
1-6	Reports and data analysis	13
1-7	IBM Intelligent Operations Center architecture	15
2-1	IBM Intelligent Operations Center servers	24
2-2	IBM Intelligent Operations Center services	26
2-3	Overall topology of the IBM Intelligent Operations Center	30
2-4	Topology of the application server	32
2-5	Topology of the event server	34
2-6	Topology of the data server	37
2-7	Topology of the management server	39
3-1	IOControl command actions and target options	45
3-2	Stopping the message bus service with IOControl	46
3-3	Querying the status of all the IBM Intelligent Operations Center servers	48
3-4	System Verification Check page	49
3-5	Available System Verification Check tests (1 of 3)	50
3-6	Available System Verification Check tests (2 of 3)	51
3-7	Available System Verification Check tests (3 of 3)	51
3-8	IOC event flow test failed	52
3-9	Problem determination procedure for IOC Event Flow failure	53
3-10	IBM Tivoli Netcool/Impact status off	54
3-11	IBM Tivoli Netcool/Impact started	54
3-12	IOC Event Flow test successful	55
3-13	IBM Intelligent Operations Center Administration Consoles	56
3-14	Starting the Application Server web-based administration console	59
3-15	Starting the Sample Event Publisher portlet	60
3-16	Test CAP event with Sample Event Publisher portlet	60
3-17	Sample Event Publisher portlet - Randomized Events	61
3-18	Test CAP event in the user interface	61
3-19	Canceling a test event	61
3-20	Generating a test KPI message	62
3-21	Test KPI message that is displayed in the user interface	63
3-22	KPI drill-down	64
3-23	Generating a test notification message	64
3-24	Test notification message in the user interface	65
3-25	Closing an alert and removing the notification from the user interface	65
3-26	Administration Consoles - Application Monitoring	66
3-27	IBM Tivoli Monitoring Service Index	66
3-28	Tivoli Enterprise Portal logon	67
3-29	False alert that is caused by a process that stops	68
3-30	Resetting critical alerts after the initial installation	69
3-31	System usage, disk I/O, and average system load	70
3-32	Log analysis for IBM Tivoli Directory Server	71
3-33	Portal server application health	72
3-34	Starting WebSphere MQ Explorer	73

3-35 IBM Intelligent Operations Center queue manager status	73
3-36 Checking the number of messages in the queues	74
3-37 Database control center view	75
3-38 Starting Tivoli Netcool/OMNIBus Administrator.	76
3-39 Connecting to NCOMS ObjectServer (1 of 2).	77
3-40 Connecting to NCOMS ObjectServer (2 of 2).	77
3-41 Browsing NCOMS databases	78
4-1 System Verification Check - list of database instance tests	87
4-2 System Verification Check tool results of the database status check.	88
4-3 Migrating a feature or change request from development or test to production environment	96
4-4 Tivoli Monitoring Service Index.	97
4-5 Tivoli Enterprise Portal navigator view	98
4-6 Tivoli Enterprise Portal physical view of Linux operating system	99
5-1 Starting the web-based console for Tivoli Access Manager.	106
5-2 Logging in to the Web Portal Manager	107
5-3 Changing the global user policy values	108
5-4 IBM Intelligent Operations Center access management overview	110
5-5 Portal view for a member of the CityWideSupervisor user group	114
5-6 Checking portal pages permissions	115
5-7 Resource permissions for Citywide portal pages	115
5-8 Searching for the Operator:Operations page	116
5-9 User access for Operator:Operations page (1 of 2)	116
5-10 User access for Operator:Operations page (2 of 2)	116
5-11 Checking user permissions.	119
5-12 User Permissions Summary portlet - Users tab	120
5-13 User Permissions Summary portlet - Summary tab	121
5-14 Starting the Tivoli Directory Server Web Administration Console.	122
5-15 Logging in to the Tivoli Directory Server Console for the first time	122
5-16 Setting up the Web Administration Tool to manage the directory server	122
5-17 Directory server login	123
5-18 Adding a user	124
5-19 Searching for the citywideoperator group	124
5-20 Adding a user to the CityWideOperator group	125
5-21 Adding user mary to the CityWideOperator group	125
5-22 Mary is a member of the CityWideOperator user role group.	126
5-23 Mary is a member of the ioc_base_transportation data category group.	126
5-24 User permissions summary for user mary	127
5-25 Editing a user profile	128
5-26 Changing a user password	129
5-27 Editing a user profile	129
5-28 IBM Intelligent Operations Center single sign-on	133
6-1 Details portlet not shown.	140
6-2 No members with a user role for portal resource - Details portlet.	141
6-3 Map and portlet applications on the Administration console.	142
6-4 System Verification Check test for db2inst1 IOCDDB service status	142
6-5 Database control center for IOCDDB database	143
6-6 CAPALERT table - events list.	144
6-7 Event services in Service Status box	146
6-8 IOC_Update_CABDB policy on event processing and enhancing system	146
6-9 NCOMS or object server cap.info table accumulated data	147
6-10 IOC.MB.QM queue manager is stopped.	147
6-11 IBM WebSphere Message Broker is not running and IOC.CAP.IN queue depth is	

increasing	148
6-12 IOC_CAP_OUT message depth is 3	149
6-13 Event cannot be submitted when the message bus is stopped	149
6-14 My Activities portlet with assigned activities	150
6-15 SOP activities that are triggered by matching SOP matrix event	151
6-16 SOP with the steps and owners assigned	153
6-17 WPSADMIN Person group that is associated with wpsadmin	154
6-18 Person is in the Active status	154
6-19 SOP associated with a SOP Matrix	155
6-20 KPI portlets on the Supervisor: Status page	157
6-21 Failed event sequences	158
6-22 Events Management display	158
6-23 KPI messages in the CAPALERT table	159
6-24 Message bus down and accumulating messages in the IOC_KPI_IN queue	160
6-25 WebSphere Business Monitor application stopped	161
6-26 NCOMS accumulation of KPI messages	164
6-27 Messages in the NOTIFICATION table	166
6-28 No resources within a 5-mile radius of the event	174
6-29 Resources found in a 100-mile radius of the event	174
6-30 Resource capabilities	175
6-31 Displaying the content of the IOC.RESOURCE table	176
6-32 Application server data sources	176
6-33 Testing a data source connection	177
6-34 IOC.CAPABILITY and IOC.CATEGORY_X_CAPABILITY table contents	177
6-35 IBM Intelligent Operations Center login failure message	179
6-36 Third-party server not responding on login	180
6-37 Connection error dialog box	181
6-38 User password expired error	181
6-39 User authentication form	182
6-40 List of IBM Intelligent Operations Center user accounts	183
6-41 Policy options for taiuser	184
6-42 No content available error	184
6-43 Portlets not visible in the IBM Intelligent Operations Center	185
6-44 Contact login portlet	185
6-45 Cognos portlet error	186
7-1 Event flow	191
7-2 KPI flow	197
7-3 Correlation flow	204
7-4 Notification flow	207
7-5 Sample resource	212
7-6 Sample capabilities	212
7-7 Resource data flow	213
7-8 User authentication and authorization flow	218
7-9 IBM Intelligent Operations Center system flow overview	220

Archived

Tables

2-1 Mapping of services to internal components of IBM Intelligent Operations Center. . . .	30
2-2 Nodes on the application server	33
2-3 Database instances and databases initially installed	38
2-4 Nodes on the management server	40
2-5 Hardware resources that were used in this project.	42
2-6 IBM Intelligent Operations Center execution environment for this project	42
3-1 Web-based administration consoles	56
3-2 IBM Intelligent Operations Center servers administrator's user IDs	58
3-3 Application server components and log files.	80
3-4 Data server components and log files.	81
3-5 Event server components and log files	81
3-6 Management server components and log files	82
4-1 Database System Verification Check tests and IOControl targets	87
4-2 Sample backup policy	89
4-3 IBM Intelligent Operations Center databases on the data server to backup.	90
4-4 Description of query commands	91
5-1 Service user IDs in the IBM Intelligent Operations Center	102
5-2 Sample IBM Intelligent Operations Center solution users.	105
5-3 Default global user policy settings	105
5-4 WebSEAL junctions and the web services they protect	111
5-5 Sample portal resources and associated user role group permissions.	112
5-6 User category group descriptions and identifiers	118
5-7 Main IBM Intelligent Operations Center security logs	135
5-8 Trace components in IBM Intelligent Operations Center	135
7-1 Full and short queue names	189

Archived

Examples

3-1	Running the mustgather.sh script	79
3-2	Results of MustGather tool	79
4-1	Sample script to automate the backup of the log files	84
4-2	Sample Logrotate configuration file	86
4-3	Using IOControl.sh to check the status of the portal database	87
4-4	Successful results after the portal database server status check	87
4-5	Script snippet of a basic connection to a database instance	89
4-6	Script snippet to prune the IOC_COMMON.EVENT database table	89
4-7	Script snippet to prune IOC.CAPALERT	89
4-8	Script snippet to prune IOC.NOTIFICATION	89
5-1	Event category example	117
5-2	Export users under subtree DN "ou=users,ou=swg,o=ibm,c=us"	131
5-3	Export groups under subtree DN "ou=groups,ou=swg,o=ibm,c=us"	132
6-1	Sample event CAP formatted XML message	139
6-2	Status for db2inst1 database	143
6-3	Message bus failure highlighted in the ioc_xml.log file	144
6-4	Duplication event sample error log	146
6-5	Unauthorized access error in ioc_xml.log	152
6-6	KPI sample message	155
6-7	KPI message in ioc_xml.log	161
6-8	KPI notification XML message	165
6-9	KPI Notification ioc_xml.log snapshot	167
6-10	Sample correlation notification XML message	170
6-11	Sample of ioc_xml.log for correlated events	171

Archived

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 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:

BladeCenter®	IBM SmartCloud™	Redbooks (logo)  ®
Cognos®	IBM®	Sametime®
CPLEX®	ILOG®	Service Request Manager®
DB2 Universal Database™	Lotus®	Smarter Cities®
DB2®	Maximo®	Smarter Planet®
developerWorks®	Netcool®	Tivoli®
Domino®	Passport Advantage®	WebSphere®
i2®	Redbooks®	

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds 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® defines a *smarter city* as one that makes optimal use of all available information to better understand and control its operations and optimize the use of resources. There is much information available from different sources. However, city officials often lack the holistic view of the city's operations that is required to respond to the citizens' needs in a timely manner and use the city resources wisely.

IBM Intelligent Operations Center delivers a unified view of city agencies, providing three primary elements for successful management of cities:

- ▶ Use information.
- ▶ Anticipate problems.
- ▶ Coordinate actions and resources.

Chapter 1 of this IBM Redbooks® publication introduces the IBM Intelligent Operations Center solution. The chapter provides a high-level overview of its features, benefits, and architecture. This information is intended for city officials and IT architects that must understand the business value of IBM Intelligent Operations Center and its architecture.

The remaining chapters of this book focus on information that help IBM Intelligent Operations Center administrators perform daily administration tasks. This book describes commands and tools that IBM Intelligent Operations Center administrators must use to keep the solution running, troubleshoot and diagnose problems, and perform preventive maintenance. This book includes preferred practices, tips and techniques, and general suggestions for administrators of IBM Intelligent Operations Center on-premises deployments.

The team who wrote this book

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



Arundhati Bhowmick is an IBM Certified IT Specialist and The Open Group Master Certified IT Specialist. She is also a board member of the IBM IT Specialist Profession and The Open Group IT Certification board. In her current position, she is a Northern Americas Senior Client Technical Professional and Solution Architect in the IBM Industry Solutions organization, in Industry Products, focused on IBM Smarter Cities® initiatives with successful client wins. Previously, she worked in various IBM niche leadership roles, most prominently as an IBM XML Parser (Xerces) designer and developer, Sensors and Actuators (RFID) subject matter expert and client advisor, and IBM Enterprise Asset Management technical consultant. She holds an MS degree in Mathematics and MTech degree in Computer Applications, both from the Indian Institute of Technology, Delhi, India.



Eduardo Francellino is a Senior Client Technical Specialist, working for IBM Brazil in the Software Group division as a Smarter Cities SME, focused on IBM Intelligent Operations Center, IBM Intelligent Transportation, IBM Intelligent Water, IBM WebSphere® Front Office, and IBM Real-Time Asset Locator. Before he joined IBM, he worked for several other companies, mainly as a software developer in various industry sectors, such as oil and gas, telecommunication, and financial markets. He holds a degree in Information Technology from Estácio de Sá University and an MBA in Software Engineering from Federal University of Rio de Janeiro.



Luis Glehn is a Software Solution Architect in IBM Brazil, currently designing solutions for different industries, such as manufacturing, energy and utilities, pharmaceutical, and government. He spent 15 years as an application engineer, supporting sales and implementation of CATIA and ENOVIA solutions in the aerospace and automotive industries. He has a degree in Mechatronics Engineering and an MBA in Product Development Management, both from Escola Politécnica da Universidade de São Paulo.



Robert Loredó is a Patent Engineer/Certified IT Specialist and Master Inventor in the Software Group division of IBM. In these roles, he developed and patented innovative ideas in emerging technologies, such as Mobile Computing, IBM Smarter Planet®, Nanotechnology, Collaboration, and Applications. In addition to this book, Robert has written numerous publications, including IBM developerWorks® articles on cross-product integration, and research papers on biotechnology and biogenetics. He holds Bachelor's and Master's degrees in Computer and Electrical Engineering from the University of Miami and is working on his PhD in Biomedical Engineering specializing in Bio-Genetics and Neurotechnology.



Pam Nesbitt is a Senior Technical Staff Member in Industry Solutions Software, Architecture, and Technical Strategy, where she provides architecture and executive oversight to solutions that use the Smarter Cities family of products, including the Intelligent Operations Center. In her tenure at IBM, Pam has held leadership technical positions in Consulting Services, IBM Tivoli® Software Development, Corporate Technology, and Industry Solutions. Ms. Nesbitt has filed over 120 patent applications with the USPTO, is a Master Inventor, and is Intellectual Property Lead for Industry Solutions. She holds a BS degree in Neurobiology from Cornell University and an MS degree in Computer Science from Cleveland State University.



Shi Wei Yu is an Industry Solution Architect in IBM China. In this role, he focuses on the support of solution delivery for IBM Smart City client wins in China. Shi Wei had 5 years of experience in IBM SOA solution play enablement for IBM SOA technical sales during his work in IBM China SOA Design Center. His areas of expertise include security, SOA, and IT Governance. He holds two Bachelor's degrees, one in Management Engineering from Beijing Institute of Machinery Industry, and one in Computer Science and Technology from Tsinghua University.

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

Sunil Mishra: We would like to give special acknowledgement to Sunil Mishra, who is a lead developer of IBM Intelligent Operations Center. Sunil was instrumental in assisting the Redbooks team with debugging problems, supporting the systems that were used for testing, reviewing content, and supporting the team in the development of this book.

Marcela Adan, Rich Conway, Debbie Landon
International Technical Support Organization, Raleigh Center

Spencer Brown
Daniel Bourque
Anthony Carrato
Chen ISSC Chen, IBM China
Mike Cooper
Vanadis Crawford
Colin Grogan, IBM Ireland
Todd Hastings
Hui Jian He, IBM China
Ann Phelan
Jason Schanuel
Jessica G. Smith
David Soroka
James Stroud
Scott Snyder

Members of the IBM Intelligent Operations Center development team

Now you can become a published author, too!

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

ibm.com/redbooks

- ▶ Send your comments in an email to:
redbooks@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

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



IBM Intelligent Operations Center overview

Acting effectively in today's world involves rapidly assimilating information from many sources, making decisions quickly, and acting in a maximally efficient manner. IBM Intelligent Operations Center was created with precisely this model as its base. It is tailored to provide city and enterprise leaders with accessible operational and progress metrics and statuses. It integrates disparate and older systems into one engine that can simplify inputs, providing a complete overview of the enterprise or city and ensuring that the correct people are alerted to anything out of the ordinary, extreme, or important. It can kick off workflows and situation management, text you when you must know something, or provide real-time situational analysis and tracking as you work through day to day issues.

The flexibility of IBM Intelligent Operations Center means that you can integrate multiple systems into one interface, removing the need to view several interfaces at once and reducing the possibility of human error. The analytics engine that drives IBM Intelligent Operations Center means that all the information received is analyzed, processed, and stored so that insights are presented rather than volumes of data. You see what is important to you.

Under the current environment of economic uncertainty, it is imperative to work smarter and do more with less. This statement especially applies to cities where budgets are stretched thin and where a lack of the appropriate infrastructure can cost lives. Smarter Cities must use information, anticipate problems, and coordinate resources. IBM Intelligent Operations Center provides a unified view of city agencies and processes, where you can predict events that affect the city and to respond in a rapid and efficient manner.

This chapter introduces the IBM Intelligent Operations Center and provides an introduction to its features, benefits, and architecture. This information is intended for city officials and IT architects that must understand the business value of IBM Intelligent Operations Center. This chapter also provides information about the scope of this book and introduces the remaining chapters.

1.1 What a Smarter City is

Smarter Cities and enterprises are ones that drive sustainable economic growth by:

- ▶ Analyzing information across agencies and departments to make better decisions
- ▶ Anticipating problems to resolve them proactively and minimize the impact of disruptions
- ▶ Coordinating resources and processes to respond to issues rapidly and operate effectively

Cities generally have advanced systems for sanitation, utilities, land usage, housing, security, transportation, and more. As shown in Figure 1-1, a *Smarter City* is one that can balance its social, commercial, and environmental needs while it optimizes the resources it has available for the benefit of its citizens. Smarter Cities increase the value to the citizens they serve in a rapidly changing economic and urban world.

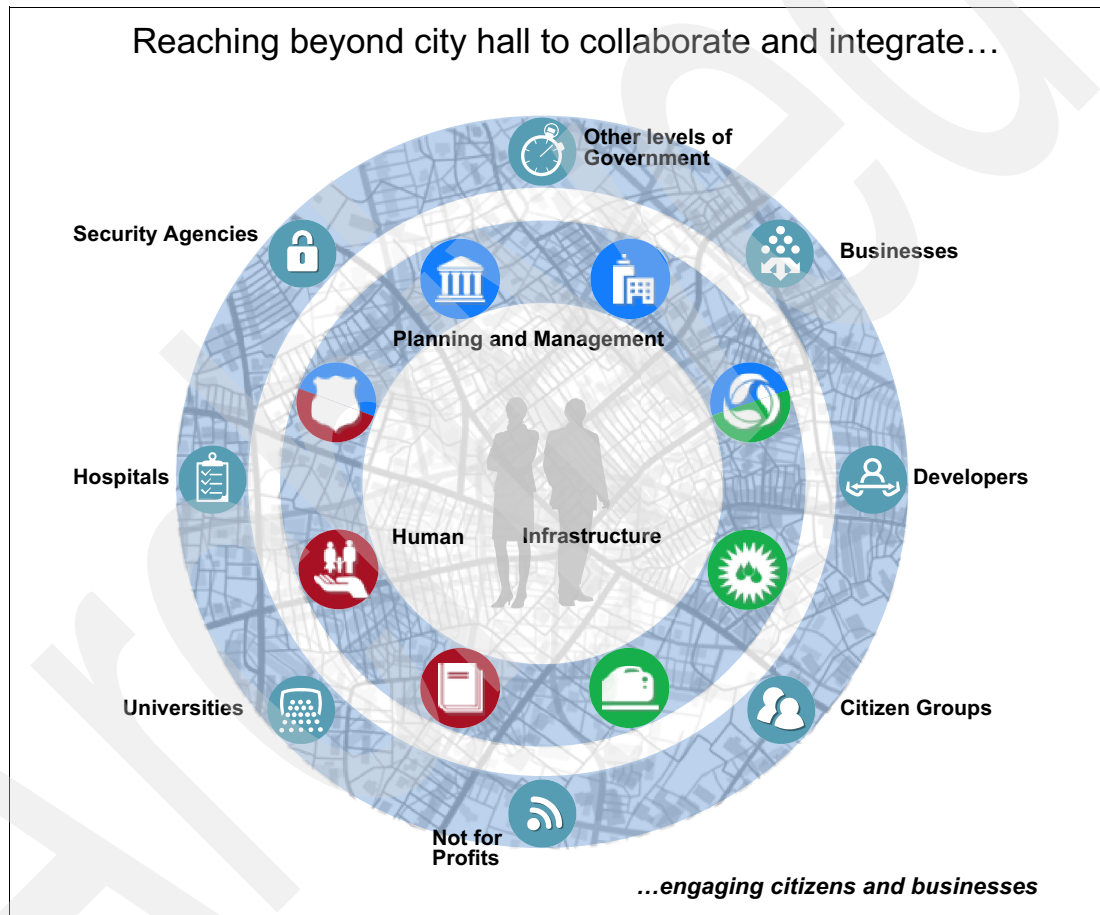


Figure 1-1 Components of a Smarter City

1.1.1 Challenges facing city leaders today

Cities around the globe are faced with the common challenges of aging infrastructures, shrinking budgets, shifting populations, and increasing threats. City executives, managers, and operators consistently report the following challenges:

- ▶ Today's cities are based on separate domains with no real ability to be managed as an entire entity.
- ▶ City managers have no single place to get real-time status or historical reports of city events.

- ▶ Older systems are domain-specific and are not concerned with the consequences on other domains.
- ▶ Daily operations of cities generate vast amounts of data from many different sources but cities often lack the ability to visualize and extract meaningful information.

IBM Intelligent Operations Center addresses these and many other challenging issues by providing insight, management, and oversight capabilities for any city or enterprise (as they both face many of the same issues).

1.2 What IBM Intelligent Operations Center is

The IBM Intelligent Operations Center solution integrates and uses data from multiple sources and makes sense of it on a single interface. It simplifies the disarray and multiplication of data sources that are necessary for understanding, yet that are too voluminous for easy consumption. IBM Intelligent Operations Center provides a single interface to all systems of an enterprise or city to make them usable without being overwhelming.

A flexible rules-based data flow directs large quantities of data into a structured format that can be used for reports and key performance indicators (KPIs). IBM Intelligent Operations Center brings events to the surface and alerts action when needed. It also provides a web-based, configurable interface that is specific to the user's role and needs so that everyone in the organization can see and collaborate on the same data in their own way. This ability to collaborate allows synchronization of effort, audit trails, collaboration, and group decision making. It also can help to synchronize and analyze efforts among sectors and agencies as they happen, giving decision makers consolidated information that helps them anticipate, rather than react, to problems.

IBM Intelligent Operations Center provides a unified view of city agencies or other complex infrastructures. It enables a city to monitor its services and operations to facilitate insightful decision-making. This approach helps provide effective event response management and coordination, from operational to critical events.

IBM Intelligent Operations Center processes data feeds and event information from individual departments to help improve the operational efficiency of a city or other complex infrastructures. It provides an executive dashboard to depict the overall status of a city's operations. The dashboard spans individual agency-specific solution areas and enables drill-down capability into each underlying agency or department. For example, water management, public safety, and traffic management.

By taking advantage of the power of advanced analytics, asset management, and collaboration tools, IBM Intelligent Operations Center delivers the ability to gain insight into an environment through centralized information.

The IBM Intelligent Operations Center capabilities include:

- ▶ Incident reporting and tracking
- ▶ Situational awareness and reporting
- ▶ Support for creating and using standard operating procedures (SOPs)
- ▶ Real-time collaboration
- ▶ Resource and critical asset management
- ▶ Assessing and displaying KPIs
- ▶ The ability to open standard connection points to existing and future systems
- ▶ An easy-to-use interface that is designed with multiple types of users in mind, from senior managers to daily operators

City and government leaders and private enterprises around the world are using IBM Intelligent Operations Center to address a broad range of management and operations needs. These needs include airport management, city operations, emergency management, energy and emissions monitoring, parks and recreation maintenance, port security, stadium operations and security, transportation awareness and prediction, and water utilities monitoring and preventive maintenance.

1.2.1 Business value

IBM Intelligent Operations Center provides the following benefits:

- ▶ Helps city officials better monitor and manage city services by providing them insight into daily city operations through centralized management and data intelligence.
- ▶ Helps city agencies prepare for problems before they arise and to coordinate and manage problems when they do arise.
- ▶ Enables officials to communicate instantly and discuss and synchronize rescue efforts so they can send the correct people and equipment to the correct places at the correct times.
- ▶ Facilitates cross agency decision making, convergence of domains, coordination of events, communication, and collaboration, which improves the quality of services to the citizens and reduces expenses.
- ▶ Flags event conflicts automatically between city agencies.
- ▶ Optimizes planned and unplanned operations using a holistic reporting and monitoring approach.
- ▶ Helps operations executive or staff to adjust systems to achieve results that are based on the insights gained.

Another major benefit of IBM Intelligent Operations Center is that it aggregates several information feeds and makes sense of them in the context of the person that is viewing them. With this capability, city leaders can quickly assess the overall status of their city or enterprise. They can swiftly identify issues that require attention and coordinate resources to respond to issues rapidly and effectively.

IBM Intelligent Operations Center can recognize events as they arise, promoting them for instantaneous response by necessary parties. It supports creating and using standard operating procedures (SOPs) in response to these events, maintaining an overall transparency for interested parties to remain apprised of progress in handling events. Having this real-time information about events and SOP responses in place allows for efficient management.

Figure 1-2 shows an Operations page from IBM Intelligent Operations Center that pulls together relevant information from various sources into one meaningful view.

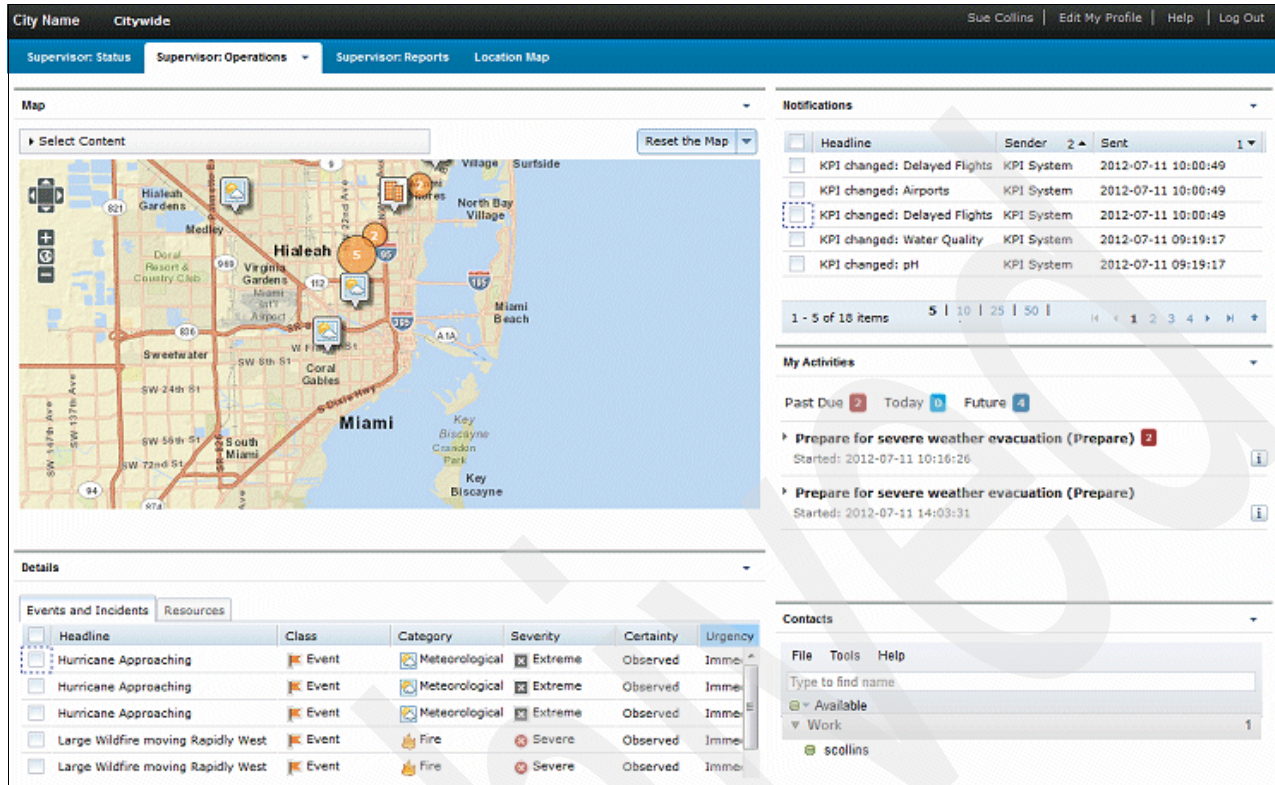


Figure 1-2 IBM Intelligent Operations Center operator dashboard

1.2.2 Key concepts

Before describing the functions provided by the IBM Intelligent Operations Center solution, it is important to explain some of the concepts that are mentioned in this section.

Events

An event is a significant occurrence or happening that is important and noteworthy to the IBM Intelligent Operations Center operations executive or staff. An event can be an occurrence at a single point in time, or it can have a duration that is associated with it. It can have a location that is associated with it, a severity, and other information about it, either collected when it was identified, or added later. Events are continually updated through time as they evolve and as more information is gathered about them and about the response to them.

Detection of events can be automated or manual. Events come into the IBM Intelligent Operations Center in different forms that are based on the nature of the operations and domains.

Here are some examples of the different types of events:

- ▶ *Triggers* are events that are generated by a real-world physical happening and usually require an action by the recipient. Examples of triggers include:
 - Fire or smoke alarms going off
 - Information technology systems going down
 - Intrusion detectors that are tripped
 - Natural events picked up by sensors, such as earth tremors

The importance of events can be filtered by the event engine so that lower-level indicators are only shown if they merit wider attention or if they represent a confluence or correlation of events in an area. For example, all fires might not be reported as events. However, a fire that involves multiple divisions of the fire service and environmental protection department, because of hazardous material, would merit an alert. Similarly, several fires in one area would be noteworthy. This correlation is performed automatically by IBM Intelligent Operations Center.

- ▶ *Threshold* events help you determine when the measurements obtained from a sensor or other source are moved outside the normal range. Basic threshold events are comparisons that compare two or more measures. They can also contribute to a trend. More sophisticated threshold events can compare measures against a threshold that is created by historical information. Examples of threshold events include:
 - Over and under temperature alarms
 - High and low water levels
 - Air quality and water purity that is breaching environmental standards
 - Excessive power consumption
 - High water levels in sewage pipes that identify potential combined sewer overflow
- ▶ *Manually entered* events complement IBM Intelligent Operations Center by augmenting the automated collection of incident and event notification and by paving the way from older reporting structures. Manual creation of events in IBM Intelligent Operations Center is a simple point and click exercise and allows creation of both emergent events that are received through a call center, planned events, and events reported through other means. This interaction with IBM Intelligent Operations Center by operators also allows the simple updating of events already in the system that is based on reported information, promotion of events to incidents, and the initiation of workflows to handle emergencies.
- ▶ *Complex* events are typically the result of a confluence of factors and possibly from a number of separate events whose occurrence at one time results in the generation of a new event. This situation underlines the flexibility of the event model in IBM Intelligent Operations Center. Events can range from simple events consumed whole from another system in the enterprise, all the way to complex derived events that represent rules-based creation of events that are based on other events.

Key performance indicators (KPIs)

A key performance indicator (KPI) is a quantifiable measure that is designed to track one of the critical success factors of a business process.

In the context of IBM Intelligent Operations Center, a KPI is a performance measurement that is used to evaluate conditions of a particular event or set of circumstances for an event.

KPIs figure prominently in the IBM Intelligent Operations Center, and are the most prominent feature on the dashboards that are typically configured for executives. They provide an at-a-glance overview of the health of an entire enterprise or city. KPIs are highly configurable, meaning that the executives that log in and see all green know that this state represents the level of health and operational stability they deem acceptable. A yellow or red status means that something occurred that is outside their comfort zone. A simple click on the unacceptable KPI provides a drill-down into the underlying conditions, which roll up into the top-level color. This way, executives can see at a glance that all is well or all is not well, how unwell (yellow versus red), and the cause for the out of norm condition.

Notifications

Notifications are items that are displayed on the IBM Intelligent Operations Center dashboard that help the operator to see what recent activity occurred. Examples of notifications include receiving new events and KPI changes.

Alerts

Alerts are notifications important enough to require operator attention. Alerts are notifications that are received when:

- ▶ Multiple events are happening in the same vicinity and at a similar time, thus indicating potential conflict or a need for coordination.
- ▶ A predefined KPI value change occurs, where the change is defined as an alert triggered by the administrator.

Common Alerting Protocol (CAP) message

IBM Intelligent Operations Center typically receives events in the Common Alerting Protocol (CAP) format. CAP is a standard protocol that was developed by OASIS for emergency management and communication. The CAP format is simple and straightforward, requiring only a few fields to be useful. The sender includes only relevant information about the event's location, severity, and any other important details.

The relative commonality and extreme extensibility of the CAP protocol make it a useful choice for interchange with the IBM Intelligent Operations Center. It is also simple to use the IBM Intelligent Operations Center enterprise service bus to map non-CAP messages into the CAP format.

Event rules

You can use the flexible event engine in IBM Intelligent Operations Center to create rules that guide the flow of data as it enters the IBM Intelligent Operations Center. Determinations about the nature of the event or data, whether it should be stored, and how it should be treated, are all part of the rules engine. These rules also can trigger SOPs, workflow, emails, and so on. Event rules can guide decisions and help achieve wanted and reasonable outcomes.

In IBM Intelligent Operations Center, one of the most common results of applying a rule to an event is to trigger an action, such as a notification. Rules and policies help make decisions about incoming and in-flight events. An example of a policy is to send an email to the city operator when a situation is detected outside the allowable KPI range.

Standard operating procedures (SOP)

A standard operating procedure (SOP) defines a sequence of activities that are triggered in response to an event whose parameters meet certain predefined conditions. In an SOP, each activity corresponds to either a manual or an automated task. A workflow can be assigned to an automated task.

It is possible to specify the order in which some or all of the activities in an SOP are run. For example, the IBM Intelligent Operations Center operator can specify that a particular activity is not started until the previous activity is completed, skipped, or signed off by a manager.

Business intelligence, analytics, and reports

IBM Intelligent Operations Center supports the historical persistence of data and information around events. This situation provides the user with the opportunity to examine performance and conditions and apply business intelligence and analytics to this data. IBM Intelligent Operations Center users can identify patterns, measure the present against past performance, improve the present operation, and even predict future performance. The historical data can be easily extracted using IBM Intelligent Operations Center reporting functions.

1.3 Solution overview

IBM Intelligent Operations Center provides integrated data visualization, real-time collaboration, and deep analytics that can help leaders prepare for problems before they arise and to coordinate and manage problems as they occur, to improve the efficiency of city operations.

IBM Intelligent Operations Center delivers the following major functions:

- ▶ Visual workspace
- ▶ Events and incident management
- ▶ Resource, response, and activity management
- ▶ Status monitoring
- ▶ Collaboration, instant notification, and messaging
- ▶ Reports
- ▶ Semantic model

Usage scenarios: The IBM Intelligent Operations Center general functions that are described in this section apply to various industries and businesses, not just cities. For information about usage scenarios, see 1.6, “Usage scenarios” on page 16.

The concepts and functions that are described in this section explain how the IBM Intelligent Operations Center solution makes supervision and coordination of complex organizations more effective. Organizations must bring together large amounts of information from multiple sources, filter and analyze the data, and develop insights to help them in decision-making. IBM Intelligent Operations Center helps you evaluate the effectiveness of the decisions and applied procedures and make improvements.

IBM Intelligent Operations Center helps organizations to:

- ▶ Handle events and alerts, in both emergencies and non-emergencies.
- ▶ Organize response teams, enabling fast and clear communications between team members.
- ▶ Define and provide standard operating procedures for handling the different situations that arise, with the correct assignments, which are based on legal requirements or historical experience.
- ▶ Track the progress of the performance of those procedures, including the results of the actions.
- ▶ Locate resources with the required capabilities to handle the events.
- ▶ Enable the continuous improvement of the organization’s services and responses.

1.3.1 Visual workspace

The IBM Intelligent Operations Center user interface is a dashboard that provides *insight* into data that is customized to a user's role and authority. This flexible view into the wealth of data that is flowing into, and stored in IBM Intelligent Operations Center, is at the heart of the solution. Its appearance is configurable and delivers exactly the data the user wants to see and is allowed to see.

The role-based context is necessary because IBM Intelligent Operations Center provides many avenues to data discovery. From the wealth of data that flows through it, IBM Intelligent Operations Center can customize and display only the information that the viewer needs and that is necessary for their role.

Figure 1-3 shows an executive dashboard in IBM Intelligent Operations Center. It is possible to use this visual workspace to work with other enterprise applications, either by having their user interfaces share the display or integrating their data into the data that is used by the Intelligent Operations Center.

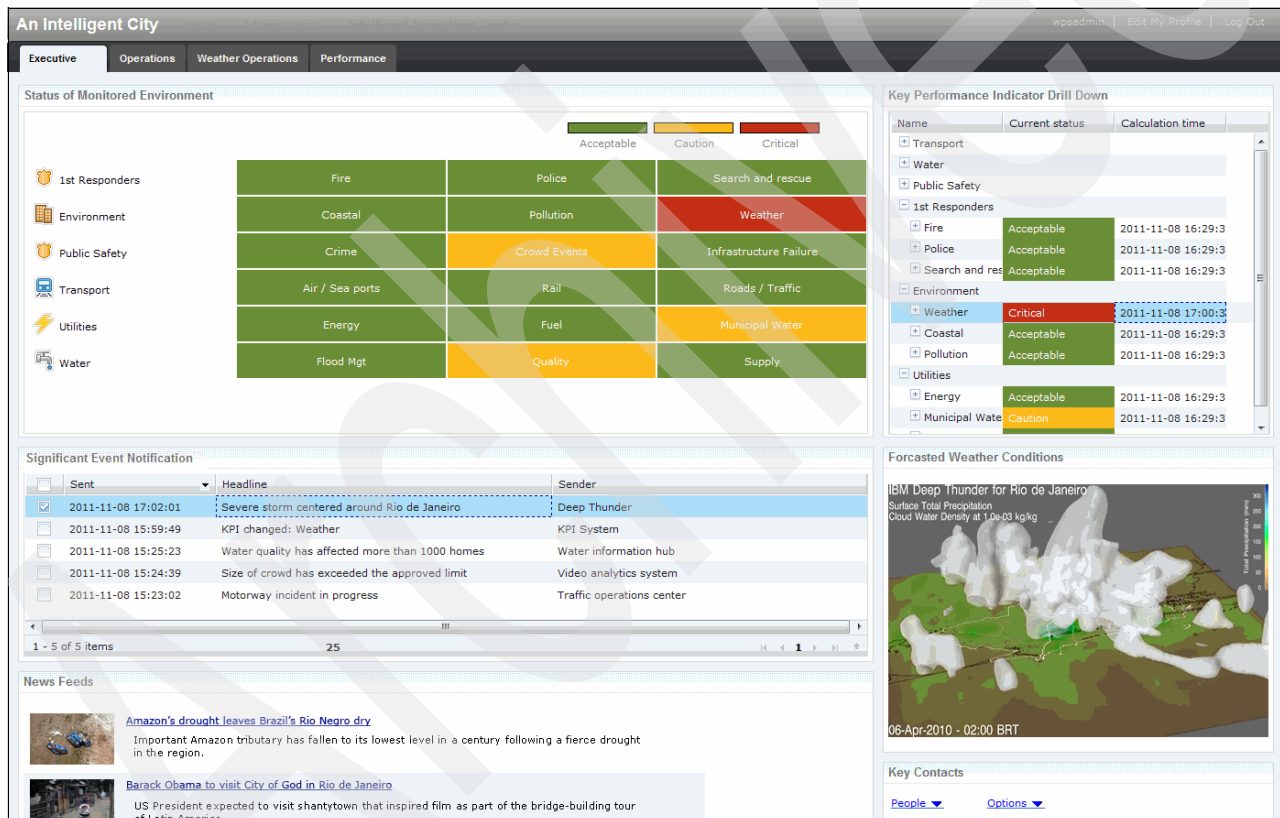


Figure 1-3 IBM Intelligent Operations Center visual workspace

1.3.2 Events and incident management

A major facet of IBM Intelligent Operations Center is its ability to use event information. Events represent occurrences of important happenings across the management domain that is represented by IBM Intelligent Operations Center. Events are presented appropriately to the user based on their role. Executives might view events as roll-ups or KPIs. Operators might see events in a list or on a map, and can respond to them based on their displayed urgency.

Events usually have temporal (point or span of time and physical (geospatial) location) attributes and a type. For example, a water main break at a particular street intersection qualifies as an event.

Events can also be things that you expect to happen in the future. Future events are useful for coordination purposes. For example, multiple city agencies might plan road work for the same section of a road at slightly different times. IBM Intelligent Operations Center can correlate the events and enable collaboration so the city tears up the road only once instead of multiple times.

IBM Intelligent Operations Center provides an event reporting and tracking mechanism to enable identification and understanding across underlying domains. You can manage predicted events, planned events, and current events as they evolve. For example, replacing pipes that run under a road is a planned event or work order that involves both water and traffic operations and possibly other operations such as cable or electric. Inclement weather due to arrive in the next 24 hours is a predicted event. A traffic jam is a current event that is affected by both the road work and weather. By managing all these types of events in one place, it is possible to improve response, reduce extra work, prepare more efficiently, and maintain a fully informed perspective of the current and future state of the enterprise.

An integrated geographic information system (GIS) or location plan maps events visually so that you can perform visual correlation, see patterns, and gauge the impact of events through interactive mapping and scenario analysis.

Figure 1-4 shows a geospatial mapping of events and an events list with detailed information about the events.

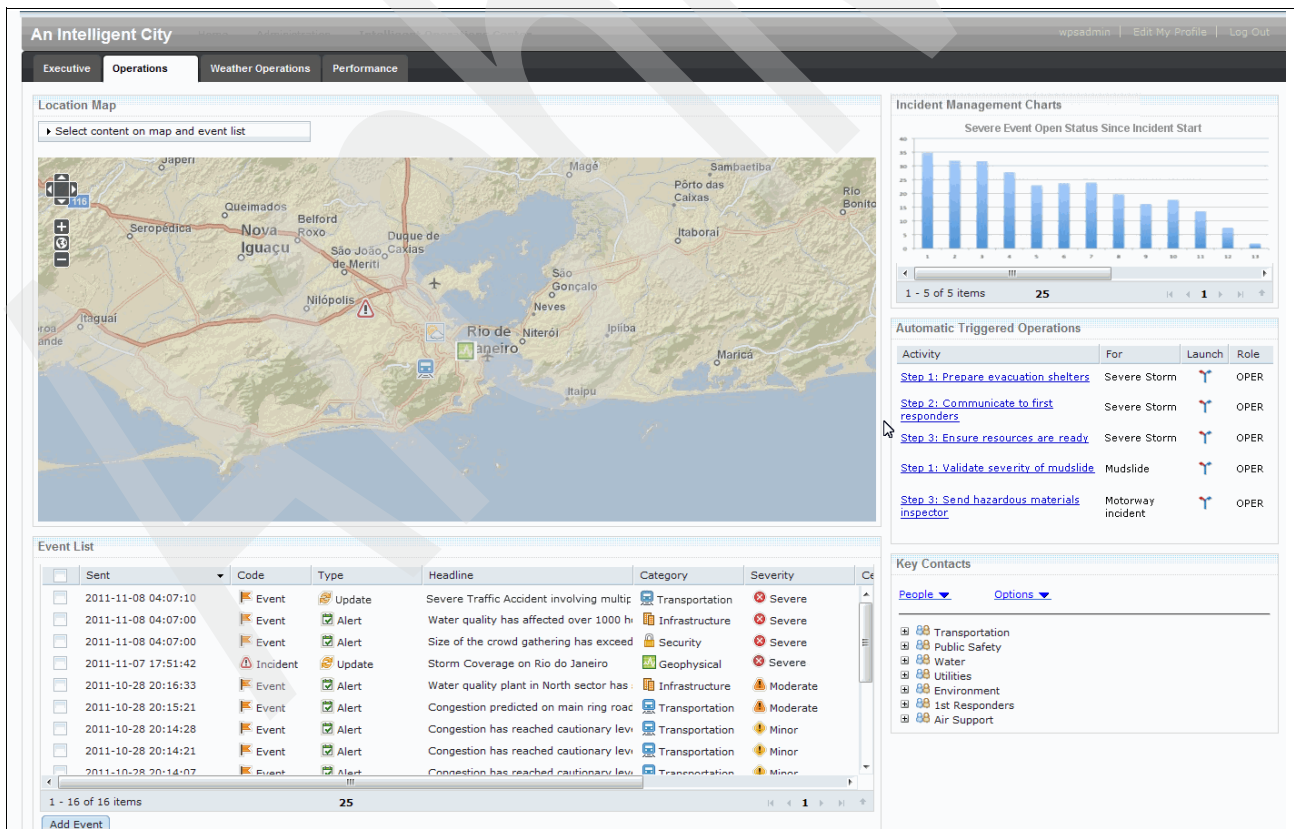


Figure 1-4 Geospatial and detailed representation of events

1.3.3 Resource, response, and activity management

IBM Intelligent Operations Center provides a system for storing appropriate procedures and workflows that are based on activities that are associated with events.

After IBM Intelligent Operations Center recognizes an event, it can choose several different actions to mediate or manage the event. Typically, a first action involves escalating the event to an *incident*. The operator might first consult SOPs and communicate with local teams through IBM Intelligent Operations Center's collaboration tools.

SOPs are predefined instructions for dealing with events or situations that a city can anticipate and plan for. SOPs can be reduced programmatically to a series of steps and actions. Some SOPs can be automated, and some require a human to make a decision.

An incident is flagged as something that requires special attention and handling. After an event is escalated to an incident, a workflow or other predefined series of actions is kicked off in accordance with an SOP.

You can track the progress of workflows and monitor or update the status of activities that are assigned to you. Information about a range of available resources can be highlighted on a map. The information is easy to access when and where you need it.

Figure 1-5 shows the list of events in the operator's dashboard and the actions that are associated with the event. For example, you can view the SOPs, find the nearby resources and their capabilities, and escalate the event to an incident.

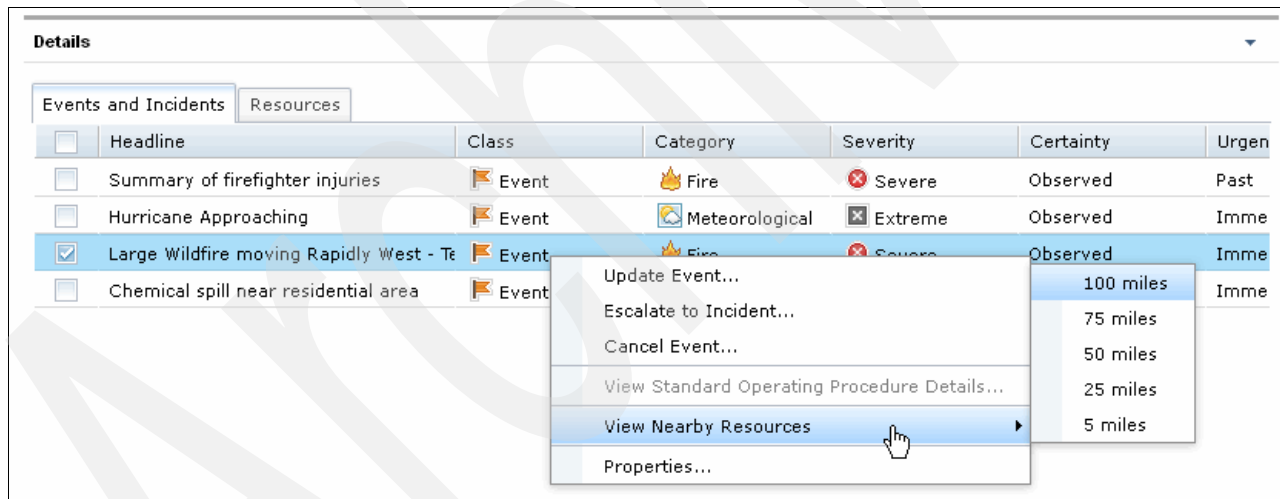


Figure 1-5 Event details and operator actions

1.3.4 Status monitoring

You can use IBM Intelligent Operations Center to tailor and define KPIs. KPIs are updated as underlying data changes. Through this function, users of IBM Intelligent Operations Center can:

- ▶ Summarize executive-level status for a single domain or across domains
- ▶ Highlight issues and identify problems
- ▶ Investigate further by drilling down into the KPI details

KPIs are used to measure nearly anything of importance to city leaders, from the number of traffic accidents this calendar quarter to the on-time performance of the public transportation system. IBM Intelligent Operations Center receives raw or computed metrics and uses them to compute the actual KPIs.

For example, for bus performance, the metrics might indicate, for each bus, whether it is ahead of schedule, on time, or behind schedule. After this information is rolled up with all the other bus information, IBM Intelligent Operations Center might create a single metric that indicates if, on average, the buses are on schedule. City bus administrators can rest easy if they see, at one glance, that the average bus arrival is green. This situation probably means that, on average, buses are arriving at approximately their scheduled times. If this KPI turns yellow or red, the administrator can determine the cause and act appropriately.

Because of the hierarchical nature of KPIs, users of IBM Intelligent Operations Center can uncover and act upon the underlying cause of the KPI change. IBM Intelligent Operations Center provides the simplicity of an overreaching and comprehensive dashboard, and the necessary underlying detail to determine a cause and enact appropriate remediation.

1.3.5 Collaboration, instant notification, and messaging

IBM Intelligent Operations Center provides a workspace where users can maintain alerts for matters that need their attention. They can use this workspace to monitor news and events, especially when other portlets that announce news are not in view.

An integrated collaboration and communication tool is also provided for messaging and communication among users where and when it is needed.

1.3.6 Reports

IBM Intelligent Operations Center has an integrated reporting facility to set up and run reports with the events and KPIs supplied by the solution. This facility collects and presents the most useful information on an up-to-the-minute and regular basis. This facility provides all the advantages of tailored summaries and graphical presentation.

IBM Intelligent Operations Center comes with a reports page that can display up to six reports. Administrators can also create a reports page manually and customize the portlet layout. The reporting subsystem uses an analytic data model. Reports can be created based on historical data that is exposed by business intelligence and analytics. Users can create *ad hoc* reports and reusable reports. Reusable reports can be easily assembled using drag-and-drop technology. They can be created as components that can be visually displayed in the IBM Intelligent Operations Center dashboard.

Figure 1-6 shows examples of reports that are built with the IBM Intelligent Operations Center reporting facility.

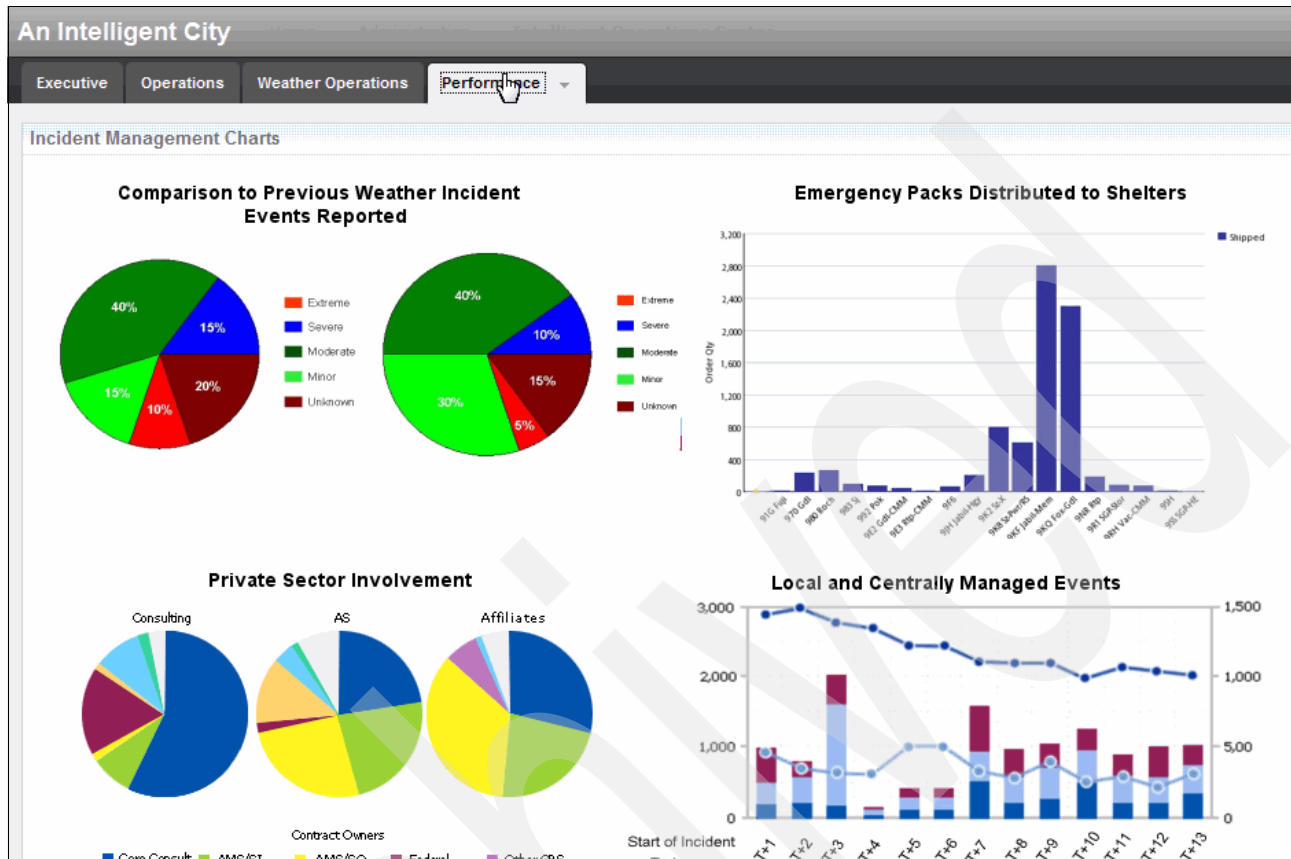


Figure 1-6 Reports and data analysis

1.3.7 Semantic model

IBM Intelligent Operations Center incorporates a hidden jewel that is known as the *model manager*. This component allows for the complex modeling of relationships in a city or enterprise between its devices, equipment, buildings, and their relationship to each other and to less palpable items, such as maintenance records, failure history, composition, and cost. This modeling and association between all the parts of a city and its processes allows for complex analysis and optimization at reduced cost and with greater ease.

As complexity increases in cities and enterprises overall, as companies acquire other companies, as utilities bring in more data sources, the need for an overarching model that can federate databases and create a single point of reference becomes essential. The reference semantic model capability that is built into IBM Intelligent Operations Center enables increasingly complex organizations to create overarching models that simplify processes, analysis, and access to relevant data.

1.4 Typical flow

The following steps describe typical flows of a message through the IBM Intelligent Operations Center solution infrastructure:

1. After IBM Intelligent Operations Center receives the CAP alert, it examines the alert and determines whether it is a *KPI* metric.
 - a. If it is a KPI metric, IBM Intelligent Operations Center forwards it to its KPI processing engine, where it evaluates the metric and updates the appropriate visual representation of the KPI.
 - b. It also sends a notification to the IBM Intelligent Operations Center user interface to notify the user about the change in the status.
2. If IBM Intelligent Operations Center recognizes a CAP alert as an *event*, it performs several actions to mediate or manage the event. Some of the actions include:
 - a. Display the event as an item in the event list.
 - b. Add an entry in the geospatial database and show the event location on the Map portlet on the operator dashboard.
 - c. Escalate the event to an incident, if appropriate.
 - d. Check the characteristics of the event against the SOP matrix, which maps event characteristics to specific procedures.
 - e. If the event matches one of the defined SOPs, a new standard operating procedure workflow is initiated and is visible in the IBM Intelligent Operations Center My Activities portlet.
 - f. Correlate events that are received within a specified time and location. For example, trigger a notification whenever two events happen within 5 miles of one another and under 2 hours between them.
 - g. Check the resources and capabilities database, link the event to the appropriate resource, and display the information in the user interface.
 - h. There are also many alternative flows that are enabled by IBM Intelligent Operations Center that allow data in various forms to be brought in over the service bus, which is interrogated by the event engine and stored or surfaced to the user interface. The rich diversity of alternatives available make the IBM Intelligent Operations Center an ideal integration platform for older and current applications, bringing together metrics, data, and alerts or events from various sources into one intuitive interface.

Resources: Resources in IBM Intelligent Operations Center are specialized assets with location and capabilities information, such as hospitals or a warehouse.

1.5 Solution architecture

Figure 1-7 provides an overview of the IBM Intelligent Operations Center architecture.

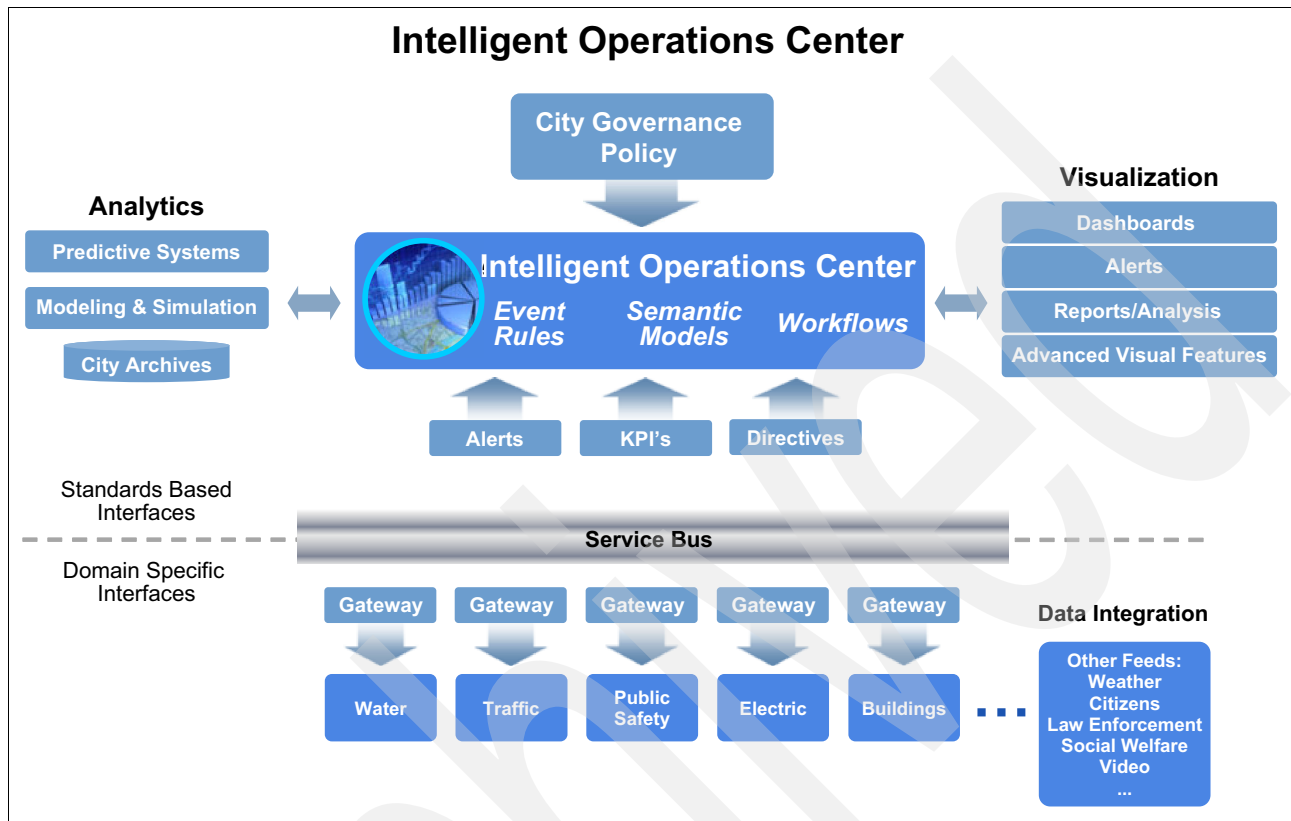


Figure 1-7 IBM Intelligent Operations Center architecture

Data from various configurable sources is received through various means (directly through XML standards-based exchange formats, or through adapters) into an enterprise service bus and world class message queuing system. This system can forward events, alerts, notifications, and KPI metrics, and initiate directives.

The IBM Intelligent Operations Center architecture has the following components:

- ▶ The *service bus* handles internal and external messages. It provides a loosely coupled interface for exchanging data and operations in a service-oriented architecture (SOA).
- ▶ The *event manager* handles anything that comes into the system, and interacts with the service bus to ensure that incoming data is treated appropriately. The event manager interrogates all incoming data and performs correlations, storage, and other activities as prescribed by the user. This flexible system can be used to apply business rules and logic to all incoming data, allowing fluid control and immediate response to critical information.
- ▶ The *KPI manager* watches all incoming data that is routed to it to continually update the KPI dashboard in accordance with user preferences. KPIs are typically viewed on the executive dashboard and provide a quick and thorough top-level status of all key processes. KPIs are tunable and can reflect the status of aggregated data, roll-up data, current versus historic performance, expenditures versus revenue, and so on. Drill down from the executive dashboard is also possible to ascertain the specific cause of a KPI changing status or color.

- ▶ The *workflows* engine helps automate and track SOPs to kickstart response to incidents automatically in accordance with a specified policy. They also afford consistency and auditability of responses, and help coordinate responses among many stakeholders.
- ▶ IBM Intelligent Operations Center is a configurable role-based interface that authenticated users can use to see the huge array of information available to them in whatever manner they find the most useful and actionable. Maps, lists, reports, and other views are user-configurable so that the users see exactly what they want to see and what they are allowed to see. Integration of outside sources of data is possible, such as video and social media.
- ▶ The *semantic model* provides an unparalleled ability to model objects in an enterprise or city and the relationships between them. This representation and the flexible ability to traverse the relationships between equipment, processes, and materials makes possible the complex analysis of the impact of device status changes on processes and things like cash flow and revenue. Semantic models can create a holistic model of multiple systems of hardware and their interrelationships and their impact and effect on business processes and non-device issues.

IBM Intelligent Operations Center takes full advantage of this capability to provide a simplified view of a complex world and analytical capabilities, which leads to unique insight. Advanced analytics can analyze the data, identifying optimizations and predictions that can help guide decisions and develop policies.

Other systems can be integrated with the solution. There are several common integration points where customizations can be done, which provide consistency. IBM Business Partners and independent software vendors (ISVs) can use these integration points and the included infrastructure services to build a powerful and broad solution that is tailored to the client's specific needs.

1.6 Usage scenarios

IBM Intelligent Operations Center-based solutions span a broad range of industries and organizations. Several use cases apply to water management, public safety, transportation, social programs, entertainment venues, buildings, energy, and more.

This section includes only a few scenarios of usage that are based on solutions that are developed with IBM Intelligent Operations Center.

1.6.1 Advanced emergency response system

In this scenario, IBM Intelligent Operations Center is used to build a city's advanced emergency response system. The city's operations center integrates information and processes from across many different city agencies into a single operations center that provides a holistic view of how the city is functioning on a 24 x 7 basis.

Business needs

Improve city safety and responsiveness to various types of incidents, such as flash floods and landslides.

Solution

An automated alert system notifies city officials and emergency personnel when changes occur in the flood and landslide forecast for the city that is based on predefined thresholds. In contrast to previous systems, where notifications are manually relayed, the new alert system should drastically reduce the reaction times to emergency situations by using instantaneous mobile communications, including automated email notifications and instant messaging, to reach emergency personnel and citizens.

The emergency management solution that is based on IBM Intelligent Operations Center:

- ▶ Integrates information from across agencies and systems
- ▶ Provides a dashboard to manage and visualize workflows
- ▶ Facilitates cross agency decision making and collaboration
- ▶ Optimizes intra-agency resource and task scheduling
- ▶ Flags event conflicts automatically between city agencies
- ▶ Efficiently controls and uses cross agency resources, thus reducing the time to resolution of emergency and crisis situations

Benefits

The emergency response system that is based on IBM Intelligent Operations Center:

- ▶ Helps save lives by enabling city officials to react and respond to disasters faster and more efficiently
- ▶ Maximizes efficiency and improves service levels that are provided to citizens

1.6.2 Wastewater management

With the IBM Intelligent Operations Center acting as the central point of command, the solution collects, analyzes, and monitors live data from sensors and level indicators in the sewer system. This setup helps control wet weather flow through the remote use of wireless sensors, smart valves and ballasts, or inflatable bands.

Business needs

A city's department of water works utility maintains a complex system of water mains, water meters, filtration plants, well fields, and water storage facilities. The system uses a combined sewer overflow model in which one large pipe carries all wastewater, storm water, sanitary sewage, and other pollutants, to the water treatment plants. In a heavy rainstorm, the city's aging infrastructure might not handle the large volumes of rainwater and wastewater. The resulting overflow of raw sewage never reaches the treatment plants and, instead, is released directly into the river, which poses significant health and property risks.

City officials are looking for a way to solve this problem and further extend and use the water system's existing data and sensor technology. They are looking for a more sophisticated and intelligent alternative to digging up the city's streets and rebuilding virtually the entire water works infrastructure.

Solution

The solution that is based on IBM Intelligent Operations Center collects information from sensors that are placed in the sewer system. These sensors proactively monitor the water flow and alert the city water authority when water is rising to dangerous levels or a blockage occurs. This sensor data can then be used to create a dashboard with geospatial mapping that shows precise "hotspots" where the risk of sewage overflow is greatest.

Key features and capabilities of the solution include:

- ▶ Overlay mapping of key data values for an at-a-glance status
- ▶ Collection system for wastewater levels and pumping station operation
- ▶ Collection of trending and historical data from water and wastewater operations for planning
- ▶ Basement backup heat map
- ▶ Calculation of combined sewer overflow volumes from supervisory control and data acquisition (SCADA) collection system wastewater levels
- ▶ System level and GIS view of cross-silo SCADA components

The solution relies on data that is collected by sensors and integration of software that is provided by IBM Business Partners. This integration is possible because of IBM Intelligent Operations Center architecture and defined common integration points.

Benefits

The city can use this solution to make proactive decisions, and initiate and monitor predefined action plans to alleviate or manage a flood threat. City operators can take proactive measures, such as deploying a crew to repair a sewer line, call in fire, police, or rescue personnel, or send an urgent alert to citizens to prevent public health disasters before they occur.

The solution helps the city to attain real business results:

- ▶ The solution cuts down on wet weather overflows and dry weather overflows.
- ▶ The city gains millions gallons of capacity in its water system.
- ▶ The city avoids millions of dollars in infrastructure investments plus more in potential government fines.

In addition to collecting and aggregating data to deliver a unified view of the combined sewer overflow infrastructure, the solution employs sophisticated analytics and monitoring capabilities that help the city predict where sewage overflow is likely to occur.

1.6.3 Entertainment venue operations center

This example focuses on an entertainment venue that must manage a continuing series of events. The venue could represent a sports complex or stadium, cruise ship, theater, or a concert hall, and the events can range from a regular schedule of games, shows, concerts, or a combination of these events.

Business needs

A major goal of entertainment venues is to improve the overall customer experience, such as getting to the stadium, ease of parking, waiting in lines, and the quality of the entertainment itself. Improving the entry and exit flow from the event is an important part of customer satisfaction.

Solution

The IBM Intelligent Operations Center solution provides an interconnected view of stadium activity, from weather alerts, to real-time security, to traffic flow into the stadium to create a seamless flow of visitors that attend a game, to insights into whether visitors prefer a full dining experience or buy food at concession stands before a big game.

Advanced crowd control management with geospatial intelligence and audiovisual notifications supports security personnel, who can immediately shift the flow of fans to minimize crowding.

Benefits

Stadium staff can now offer a unique fan experience by enabling event specialists to more effectively manage visitor traffic, monitor inclement weather, and analyze visitor spending habits on concessions, merchandise, and dining services to better target the fans with premium products and services.

Real-time analysis also enables staff to predict consumer preferences and plan concession and merchandise needs for current or future events. For example, as concession and dining service sales contribute a significant amount of revenue for a stadium, anticipating a fan's preference for a full dining experience or purchasing food at a concession stand during an event is key to increasing business profitability.

1.7 New features of IBM Intelligent Operations Center V1.5

IBM Intelligent Operations Center V1.5 introduces useful new features:

► Report enhancements

Users can use a configurable reporting capability to set up reports to gain insight into decision grade information that is captured by IBM Intelligent Operations Center. Twenty-four sample reports are now included.

In the new Reports portlet, users can:

- View up to six reports of events as graphs.
- Create custom reports that are based on selected criteria and data, including reports for events by date or date range.
- Copy a report URL and have the report display in a frame to the right of the portlet.

► Workflow enhancements

Users can select the most appropriate response to an event captured by IBM Intelligent Operations Center. Users can track the status of activities that are associated with events. In the new My Activities portlet, users can:

- View a group's open tasks that are associated with a procedure and an event.
- View the status of tasks that are assigned to them.
- Change the status of tasks that are assigned to them.

► Simplified configuration and customization

Handling of KPIs, SOPs, rules, and workflows for specific environments is aimed at business analysts, which helps reduce the need for dedicated IT staff to assist with these activities.

► Resource management and location map enhancements

In the new Location Map and enhanced Map portlets, users can:

- Assess the resources available to them in the vicinity of an event that is based on a geographical map.
- Work with a new type of map, a location map, with interactive areas defined. For example, a location map can be based on plan of routes for a transport system.
- View more than one event that is clustered at the same location on a map.

- ▶ Installation enhancements

The IBM Intelligent Operations Center environment is deployed on four virtual machines (VMs) (down from seven VMs in Version 1.0).

- ▶ Portlet customization enhancements

With the new portlet configuration options, administrators can set the following properties for each portlet:

- Properties that are specific to individual portlets. For example, set the center point and zoom level for a map.
- Properties that are generic across portlets. For example, set the portlet height.

- ▶ New administration tools

- System Verification Check Tool: Administrators can use the System Verification Check Tool to check the operational status of IBM Intelligent Operations Center.
- Event Scripting portlet: Administrators can use the new Event Scripting portlet to create a sequential list of events to be published at predefined time intervals.

- ▶ New supported protocols

IBM Intelligent Operations Center now supports events with protocols other than the Common Alerting Protocol. Event messages can now be in custom (non-CAP) formats. Administrators can:

- Extend enumerated types for Common Alerting Protocol and non-Common Alerting Protocol events.
- Customize the pop-up menus in the Details portlet.
- Accept events from multiple domains for display in portlets.

- ▶ New connection points to integrate more applications

IBM Intelligent Operations Center includes additional connection points to new applications found in the Smarter Cities application store. These applications can act as additional data sources. Applications currently available within the application store that can be connected to the Intelligent Operations Center include:

- City Pulse: Allows the general public to report issues through mobile services requests.
- Mayor's Dashboard: Provides an easy-to-read dashboard for executives to view issues in their city.
- Sentiment Analysis: Learns what citizens are saying through social media forms about city services and policies.
- SOP for Emergency Management: Allows trained personnel to react to emergency situations using defined SOPs.
- Weather for Operations: Delivers accurate weather forecasts and the ability to predict adverse weather conditions.
- Resource Management for Emergencies: Collects information about the condition of assets that are used during emergency situations.
- Smarter Stadiums: Provides situational awareness and actions to maximize stadium operations and stadium revenue sources.

- ▶ Connection to related IBM solutions

IBM Intelligent Operations Center base can connect to a selection of related IBM solutions:

- IBM i2® Public Safety
- Smarter Buildings

- Video Correlation and Analysis Suite (VCAS).
- ▶ Support for a multilingual customer user interface for operational tools

The IBM Intelligent Operations Center is now central to its associated products, which include Intelligent Water and Intelligent Transportation. Therefore, the features and functions that are present in the IBM Intelligent Operations Center are also available in the Intelligent Water and Intelligent Transportation products.

1.7.1 Supported platforms

IBM Intelligent Operations Center can be deployed within a city's data center (on-premises) and through a subscription service hosted on the IBM SmartCloud™.

For city managers that prefer a subscription service model that does not require more hardware or IT management capacity, IBM Intelligent Operations Center on IBM SmartCloud is an ideal solution. This service provides rapid and secure internet access to the capabilities of the IBM Intelligent Operations Center on IBM SmartCloud so cities can rapidly adopt new capabilities while they control cost. For more information, see IBM Smarter City Solution on Cloud at:

<http://www-01.ibm.com/software/industry/smartercities-on-cloud/>

For on-premises deployments, IBM Intelligent Operations Center requires five 64-bit x86 servers. Red Hat Enterprise Linux Version 5, Update 5 or later must be installed on all servers. For information about minimum hardware requirements, see the “IBM Intelligent Operations Center hardware requirements” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/ba_plan_hardware_lite.html

1.7.2 Ordering information

IBM Intelligent Operations Center is only available through IBM Passport Advantage®. It is not available as a shrink-wrapped product. Following are the product specifics:

- ▶ Product Group: Smarter Physical Infrastructure
- ▶ Product identifier: 5725-D69
- ▶ Product identifier description: IBM Intelligent Operations Center
- ▶ Product Category: Smarter Cities
- ▶ Charge metric: User Value Unit (UVU)

1.7.3 Related information

For more information about IBM Intelligent Operations Center, see the following documents:

- ▶ IBM Intelligent Operations Center V1.5 announcement letter:
<http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS212-250&appname=USN>
- ▶ IBM Intelligent Operations Center Product page:
<http://www-01.ibm.com/software/industry/intelligent-oper-center/>
- ▶ IBM Intelligent Operations Center Information Center:
<http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/index.jsp>

- ▶ Solutions for Smarter Cities application store:

https://www-304.ibm.com/sales/gss/download/industry_solutions_catalog/CrossIndustrySolutions.do?industry=cities

1.8 Scope and content of this publication

The focus of this publication is the daily administration tasks that IBM Intelligent Operations Center administrators must perform to administer the IT environment for on-premises deployment of the solution. Activities involving installation, configuration, and customization are outside the scope of this book.

This book includes the following chapters:

- ▶ Chapter 2, “Topology” on page 23 describes the IBM Intelligent Operations Center architectures, topology, hardware, and software.
- ▶ Chapter 3, “Administration fundamentals” on page 43 describes the basic tools available to IBM Intelligent Operations Center administrators to perform daily operations and diagnose problems.
- ▶ Chapter 4, “Preventive maintenance” on page 83 provides information about basic administrative tasks that IBM Intelligent Operations Center administrators must perform at regular intervals to keep the solution infrastructure healthy.
- ▶ Chapter 5, “Security considerations” on page 101 provides information about simple security administration tasks that administrators perform frequently.
- ▶ Chapter 6, “Troubleshooting” on page 137 explains how to identify and resolve some common problems users might experience when they are using the IBM Intelligent Operations Center.
- ▶ Chapter 7, “Data flows” on page 189 describes the main flow of messages through the IBM Intelligent Operations Center topology. Administrators can use these data flows to understand normal operations and also to help debug problems.



Topology

This chapter describes the IBM Intelligent Operations Center environment.

Topics that are covered in this chapter include:

- ▶ High-level architecture
- ▶ System topology
- ▶ Hardware and software environment that is used in this publication

2.1 High-level architecture

This section describes the overall architecture of the IBM Intelligent Operations Center solution. The architecture is presented at two levels of abstraction:

- ▶ Servers overview: A high-level overview of the servers
- ▶ Services overview: An overview of the functions and capabilities available on each server

2.1.1 Servers overview

IBM Intelligent Operations Center is composed of five logical servers:

- ▶ Application server
- ▶ Event server
- ▶ Database server
- ▶ Management server
- ▶ Installation server

The virtual machines are spread across one to many physical servers that depend on the capacity of the physical servers and the workload of the solution.

Figure 2-1 shows the servers topology for IBM Intelligent Operations Center V1.5.

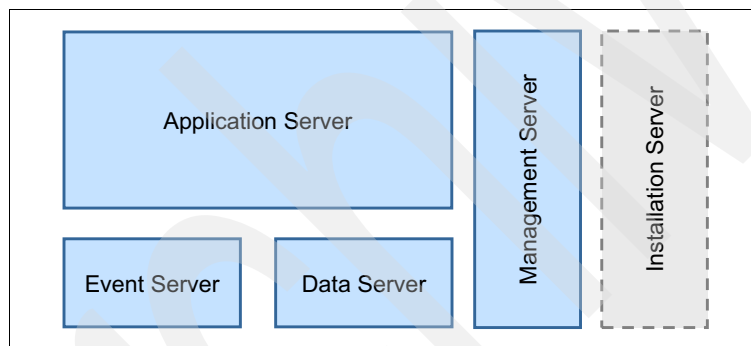


Figure 2-1 IBM Intelligent Operations Center servers

Here is a brief description of each of the servers that are shown in Figure 2-1:

- ▶ Application server: The application server is responsible for the overall web infrastructure for running the IBM Intelligent Operations Center solution. It is also responsible for the user interface infrastructure, including the display of key performance indicators (KPIs) in dashboards and report generation. It is through the application server that users log in to the IBM Intelligent Operations Center and obtain access to the entire set of functions available in the solution.
- ▶ Data server: The data server provides the data services infrastructure and repository that is used by the other internal subsystems of the IBM Intelligent Operations Center. It also holds the directory repository that is used for securing access to the different functions in the IBM Intelligent Operations Center.
- ▶ Event server: The event server is responsible for connecting with external data sources, processing incoming events, and managing the entire incident response process, which includes workflows to implement standard operating procedures and the instant messaging infrastructure to allow users to collaborate during an incident or a crisis.

- ▶ **Management server:** The management server provides the capabilities to monitor the infrastructure that is used by the IBM Intelligent Operations Center, which includes items such as hardware, operating system, databases, and the web infrastructure. The management server provides the capability to ensure that the entire IBM Intelligent Operations Center solution is performing as it should. The management server also implements key security functions that are used by the other servers in the solution, such as user access and identity management.
- ▶ **Installation server:** The installation server is used for installing the product, for applying fixes, and for some problem determination activities. It is not required for normal operations of the IBM Intelligent Operations Center.

IBM Intelligent Operations Center also requires a mapping service that is provided by a Geographic Information System (GIS). This service is not included in the solution. IBM Intelligent Operations Center uses the GIS as the map infrastructure for the map portlet and adds a specific set of icons that are used to represent different categories of events.

The IBM Intelligent Operations Center installation sets the public ESRI service and uses it to configure the GIS service. If the customer wants to use a private ESRI service, the GIS service must be configured after the initial installation.

ESRI service: ESRI is a software development and services company that provides GIS software and geodatabase management.

Each of the IBM Intelligent Operations Center servers can be installed in either a physical or virtual machine. For details about the environment that is used in the development of this book, see 2.3, “Hardware and software environment that is used in this publication” on page 41. System requirements information can be found in the “Preparing for installation” topic in the IBM Intelligent Operations Center V1.5 Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/install_pre.html

2.1.2 Services overview

Each the servers that are described in 2.1.1, “Servers overview” on page 24 provides a specific set of services. Figure 2-2 presents which services run on each of the IBM Intelligent Operations Center servers. For details about the overall topology of the IBM Intelligent Operations Center and its software components, see 2.2.1, “Topology overview” on page 30.

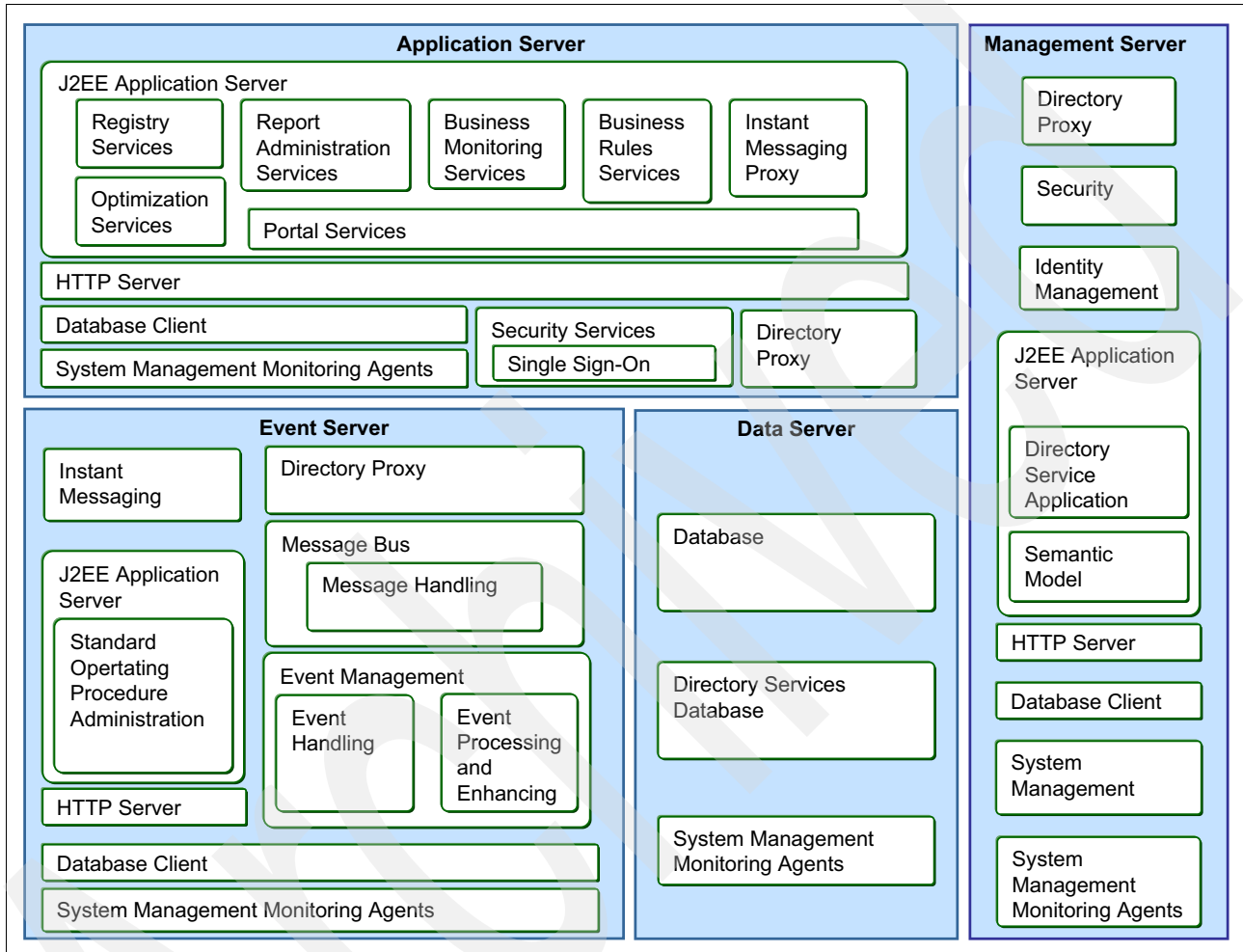


Figure 2-2 IBM Intelligent Operations Center services

Application server services

This section provides a brief description of the IBM Intelligent Operations Center system services that run on the application server:

- ▶ **Application server:** Provides Java Enterprise Edition services that support the product. It provides a J2EE platform to run applications in a web operating environment. This platform supports other components of the IBM Intelligent Operations Center, such as the portal services or the standard operating procedure administration services.
- ▶ **Registry:** The registry services are implemented by the Universal Description, Discovery, and Integration (UDDI) open standard, which allows applications to search and find web services in a dynamic way. The detailed specification of the UDDI standard can be found at the Oasis open standards website at:

<https://www.oasis-open.org/standards#uddiv3.0.2>

- ▶ **Report administration:** Provides tools for generating and managing customized reports.

- ▶ **Business monitoring:** Provides aggregation, analysis, and presentation of business process and activity information in real time. The business monitoring services are responsible for providing KPIs and metrics calculation and visualization.
- ▶ **Business rules:** Provides the rules management engine that is used for KPIs calculation.
- ▶ **Portal:** Provides services that support user interaction with the product. The portal services implement the user interface for the IBM Intelligent Operations Center.

The following supporting services also run in the application server:

- ▶ **Security services for single sign-on:** This service is also referred to as access management. It implements the single sign-on (SSO) functionality to make access to the underlying technology transparent for users.
- ▶ **Directory proxy:** Provides an interface between the application server in each server and the directory in the data server. It allows the application server to abstract the location of the directory, as it must send its requests only to the directory proxy server. The proxy reroutes the request to the correct directory. You can configure other directory servers that could be used for load balancing or fail-over purposes.
- ▶ **HTTP server:** Provides the capability to deliver web pages to client browsers. In the IBM Intelligent Operations Center, it functions as the basic infrastructure required by the application server to communicate with the web browsers that run on client desktops.
- ▶ **Database client:** Provides the connection to the database server.
- ▶ **Monitoring agents:** Part of the system management services.

For details about the topology of the application server, see 2.2.3, “Topology of the application server” on page 32.

Event server services

This section provides a brief description of the IBM Intelligent Operations Center system services that run on the event server.

- ▶ **Standard operating procedure administration:** Provides the standard operating procedures management infrastructure, including the workflow and resource management capabilities.
- ▶ **Event handling:** Collects, aggregates, presents, and handles system events. Provides event filtering and deduplication capabilities using configured policies. It uses a lightweight agent, called a *probe*, to monitor and capture incoming events in the message queue.
- ▶ **Event processing and enhancing:** Applies configured policies to incoming events, enriching the event with correlated information from other components of the IBM Intelligent Operations Center.
- ▶ **Message bus:** Allows data and information, in the form of messages, to flow between external applications and the IBM Intelligent Operations Center. Business rules can be applied to the data that is flowing through the message bus to route, store, retrieve, and transform the information.
- ▶ **Messaging handling:** Provides message and workflow services to the product. It provides queue management and the messaging transport infrastructure to allow the secure and reliable delivery of messages.
- ▶ **Instant messaging server:** Provides real-time collaboration capabilities for users and applications. It provides the collaboration infrastructure for users to communicate through instant text messages. The user connections to the instant messaging server are managed by a multiplexing service that is installed on the application server.

The following supporting services also run in the event server. For a description of these services, see “Application server services” on page 26.

- ▶ Directory proxy
- ▶ HTTP server
- ▶ Database client
- ▶ Monitoring agents

For details about the topology of the event server, see 2.2.4, “Topology of the event server” on page 34.

Data server services

This section provides a brief description of the IBM Intelligent Operations Center system services that run on the data server:

- ▶ **Database:** Provides the database manager for application and system data. The database services provide the underlying relational database capabilities that are needed to support the storage and retrieval of data by the IBM Intelligent Operations Center internal components. Multiple database instances are implemented and integrated to the other components of the solution, including the following components:
 - Business rules
 - Portal
 - Report administration
 - Business monitoring
 - Standard operating procedure administration
 - Semantic model
 - Identity management

The database client service provides the connection to the database server.

- ▶ **Directory:**
 - The directory service provides the mapping between names and values. Data services are used as a repository for user names and passwords. It provides a Lightweight Directory Access Protocol (LDAP) infrastructure that is the foundation for deploying the identity management capability within the IBM Intelligent Operations Center.
 - The directory proxy services provide an interface between the application server in each server and the directory in the data server. It allows the application server to abstract the location of the directory, as it must send its requests only to the directory proxy server. The proxy reroutes the request to the correct directory. This configuration allows for the configuration of other directory servers, which could be used for load balancing or fail-over purposes.

Additionally, the monitoring agents supporting service is also running on the data server.

For details about the topology of the data server, see 2.2.5, “Topology of the data server” on page 37.

Management server services

This section provides a brief description of the IBM Intelligent Operations Center system services that run on the management server.

- ▶ **System management:** Monitors the health, availability, and performance of the infrastructure that supports the IBM Intelligent Operations Center. It uses monitoring agents that are installed on each server to collect data on the different attributes that are monitored on each server. This data is sent to a central monitoring console of the IBM Intelligent Operations Center in the management server.
- ▶ **Security services for access management:** Provides a centralized authentication and authorization capability for controlling user access to the IBM Intelligent Operations Center.
- ▶ **Identity management:** Provides an automated, policy-based way to manage user access across the IBM Intelligent Operations Center components. By using roles, accounts, and access permissions, it automates the creation, modification, and termination of user privileges throughout the entire user lifecycle.
- ▶ **Semantic model services:** Provides services that allow applications to model real world objects and relationships. The semantic model is an abstract representation of the equipment, processes, and materials of the physical world, making it possible to standardize analytics, metrics, and business processes across disparate systems.
- ▶ **Directory services application:** The directory services provide an LDAP infrastructure that is the foundation for deploying the identity management capability within the IBM Intelligent Operations Center.
- ▶ **Database:** Database services with a separate instance to specifically support the system management services that run in this server.

The following supporting services also run in the management server. For a description of these services, see “Application server services” on page 26.

- ▶ Directory proxy
- ▶ HTTP server
- ▶ Database client
- ▶ Monitoring agents

For details about the topology of the management server, see 2.2.6, “Topology of the management server” on page 39.

2.2 System topology

This section describes the main components of the IBM Intelligent Operations Center solution and what runs on each node. It also provides an explanation of the main tools and consoles available on each server.

2.2.1 Topology overview

Figure 2-3 presents the overall topology of the IBM Intelligent Operations Center and its software components. Each of the services that are presented in 2.1.2, “Services overview” on page 26 are implemented by a software component.

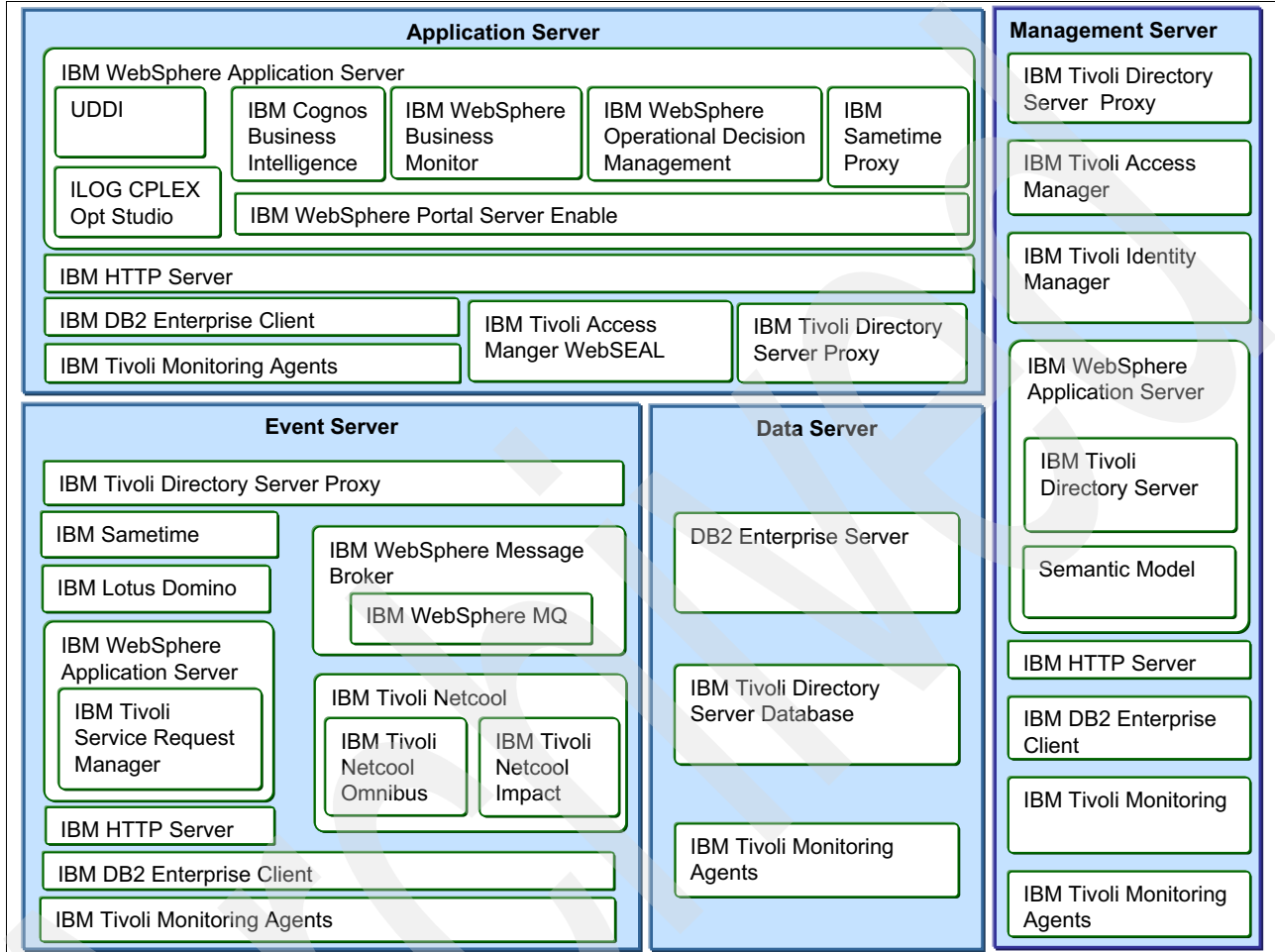


Figure 2-3 Overall topology of the IBM Intelligent Operations Center

Table 2-1 lists how each service described in 2.1.2, “Services overview” on page 26 relates to the internal components of the IBM Intelligent Operations Center.

Table 2-1 Mapping of services to internal components of IBM Intelligent Operations Center

Service	Component	Version
Business monitoring	IBM WebSphere Business Monitor	7.5
Business rules	IBM WebSphere Operational Decision Management	7.5
Contacts	IBM Lotus® Domino®	8.5.3.1
Database	IBM DB2® Enterprise	9.7.0.5
Directory	IBM Tivoli Directory Server	6.3.0.8
Event handling	IBM Tivoli Netcool/OMNibus	7.3.1.2

Service	Component	Version
Event processing and enhancing	IBM Tivoli Netcool/Impact	5.1.1.1 + IF003
HTTP server	IBM HTTP Server	7.0.0.21
Identity management	IBM Tivoli Identity Manager	5.1
Instant messaging	IBM Sametime®	8.5.2 + IFR1
J2EE application server	IBM WebSphere Application Server Network Deployment	7.0.0.21
Message bus	IBM WebSphere Message Broker	8.0
Messaging handling	IBM WebSphere MQ	7.0.1.7
Optimization	IBM ILOG® CPLEX® Optimization Studio	12.4
Portal	IBM Portal Server Enable	7.0.0.2
Registry	UDDI ^a	n/a
Report administration	IBM Cognos® Business Intelligence	10.1.1
Security	IBM Tivoli Access Manager	6.1.1.4
Semantic model	Semantic Model Services	1.5
Standard operating procedure administration	IBM Tivoli Service Request Manager®	7.2.1.2
System management	IBM Tivoli Monitoring IBM Tivoli Composite Application Manager	6.2.2.1 7.1

a. Included with IBM WebSphere Application Server Network Deployment.

2.2.2 Elements common to all servers

The following elements are supporting components of the IBM Intelligent Operations Center and are present on more than one server:

- ▶ IBM Tivoli Monitoring agents: IBM Tivoli Monitoring agents (also known as *monitoring agents*) are installed on systems or subsystems that require data collection and monitoring. The agents are responsible for data gathering and distribution of attributes to the monitoring servers. These agents test attribute values against a threshold and report these results to the monitoring servers. The Tivoli Enterprise Portal displays an alert icon when a threshold is exceeded or a value is matched. The tests are called situations.

These agents are part of the system management services and are present on all servers of the IBM Intelligent Operations Center solution. However, each server has a different set of agents.
- ▶ IBM DB2 Enterprise client: This component provides client access to the database server. It is part of the DB2 Enterprise product and is present on the application server, event server, and management server.

- ▶ **IBM HTTP Server:** This component implements the web server and is part of the IBM WebSphere Application Server Network Deployment product. It is present on the application server, event server, and management server.
- ▶ **IBM Tivoli Directory Service Proxy:** This component provides client access to the directory service and is part of IBM Tivoli Directory Server. It is present on the application server, event server, and management server.

2.2.3 Topology of the application server

This section presents the detailed topology of the application server. Figure 2-4 shows an overview of the application server topology.

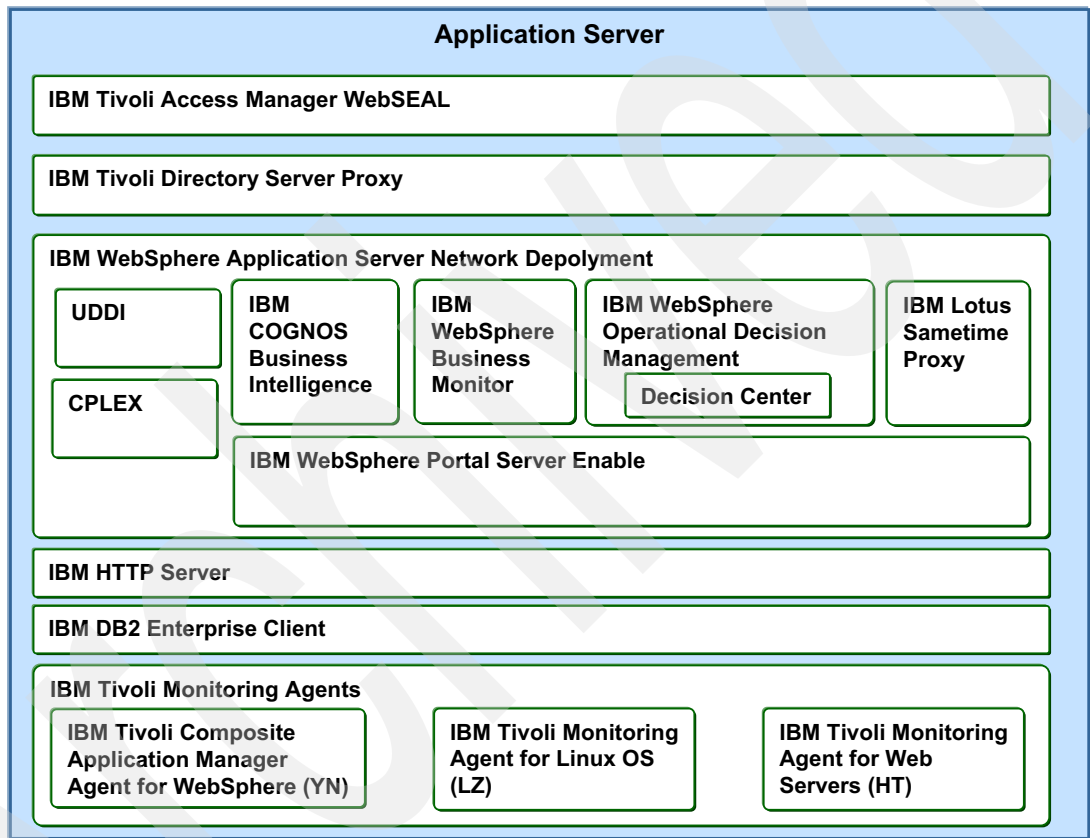


Figure 2-4 Topology of the application server

IBM WebSphere Application Server Network Deployment

The IBM WebSphere Application Server provides the runtime environment where the different components of the IBM Intelligent Operations Center run. It uses a logical organization that is based on nodes and implements the application server services that are described in 2.1.2, “Services overview” on page 26.

Note: A node is an administrative grouping of application servers for configuration and operational management within one operating system instance.

The IBM Intelligent Operations Center has several nodes that are initially configured on the application server. Table 2-2 lists these nodes, what application they are running, and what service is being implemented.

Table 2-2 Nodes on the application server

Application server name	Node name	Application	Service implemented
CognosX_Disp1 CognosX_GW1	CognosNode1	IBM Cognos Business Intelligence	Report administration service.
WebSphere_Portal	PortalNode1	IBM WebSphere Portal Server Enable	Portal service.
STProxyServer1	STProxyNode1	IBM Sametime Proxy	Implements the user multiplexing capabilities to the instant messaging server service.
WBM_DE.AppTarget. WBMNode1	WBMNode1	IBM WebSphere Business Monitor	Business monitoring service.
wodmServer1	WODMNode1	IBM WebSphere Operational Decision Management	Business rules service.
wodmdc1	wodmdcNode	IBM WebSphere Operational Decision Management Decision Center	Part of the business rules engine. Its purpose is to provide a user environment for editing the rules.
cpudServer1	cpudNode1	IBM ILOG CPLEX Optimization Studio (CPLEX) Universal Description, Discovery, and Integration (UDDI)	<ul style="list-style-type: none"> ▶ CPLEX includes CPLEX Optimizer and CPLEX CP Optimizer. It provides a platform for developing and deploying optimization models. ▶ UDDI implements the registry services.

IBM Tivoli Access Manager WebSEAL

The Tivoli Access Manager is part of the security services and implements the single sign-on capabilities in the IBM Intelligent Operations Center.

IBM Tivoli Monitoring agents

The following monitoring agents are installed on the application server:

- ▶ IBM Tivoli Composite Application Manager Agent for WebSphere (also known as YN): This agent collects and forwards monitoring information about the performance of the application server to the Tivoli Enterprise Monitoring Server on the management server.
- ▶ IBM Tivoli Monitoring Agent for Linux OS (also known as LZ): This agent collects and forwards monitoring information about the performance of the Linux operating system to the Tivoli Enterprise Monitoring Server on the management server.
- ▶ IBM Tivoli Monitoring Agent for Web Servers (also known as HT): This agent collects and forwards monitoring information about the performance of the HTTP server to the Tivoli Enterprise Monitoring Server on the management server.

2.2.4 Topology of the event server

This section presents the detailed topology of the event server. Figure 2-5 shows an overview of the event server topology.

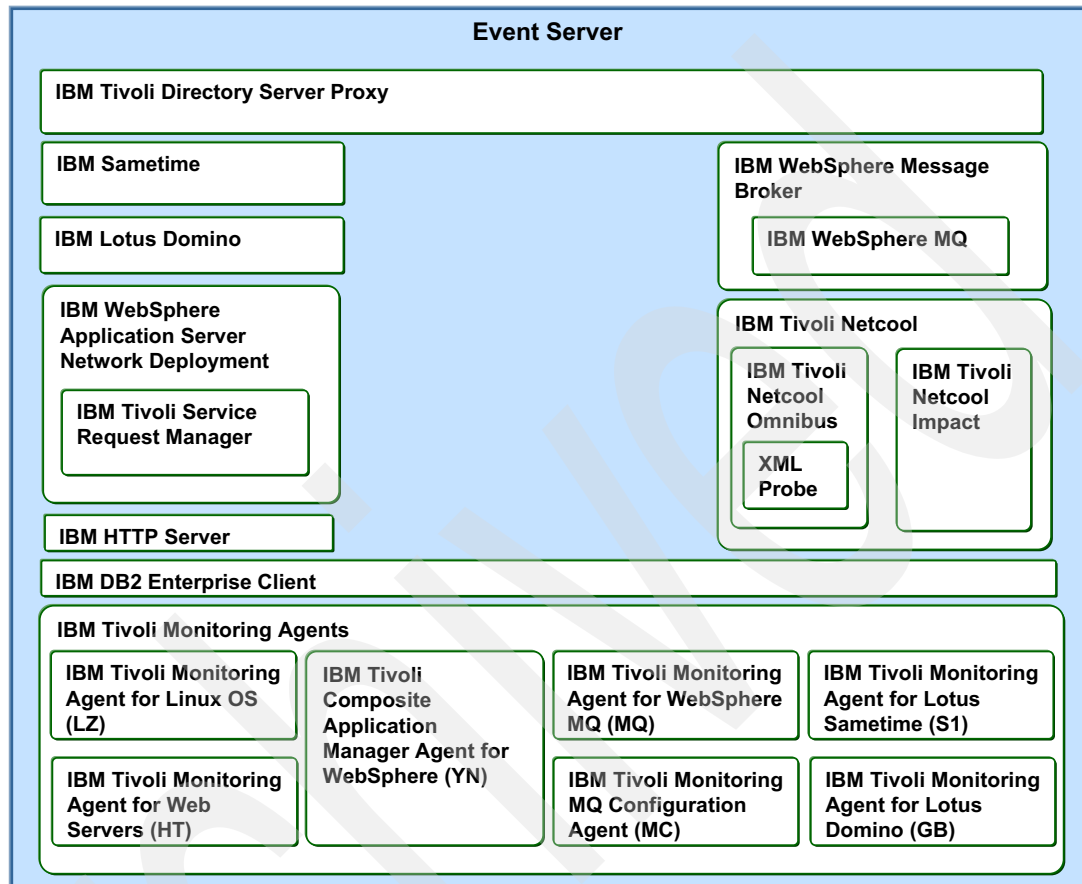


Figure 2-5 Topology of the event server

IBM WebSphere Application Server Network Deployment

The IBM WebSphere Application Server provides the runtime environment where the different components of the IBM Intelligent Operations Center are run. It uses a logical organization that is based on nodes and implements the event server service, as described in 2.1.2, "Services overview" on page 26.

Note: A node is an administrative grouping of application servers for configuration and operational management within one operating system instance.

The IBM Intelligent Operations Center has several nodes that are initially configured on the event server. The main node for administration is ctgNode01, whose application server name is MXServer1. This node runs the IBM Tivoli Service Request Management application, which implements the standard operating procedure administration service.

IBM WebSphere MQ

IBM WebSphere MQ provides a robust messaging integration platform that is based on queues. Its publish and subscribe mechanism allows asynchronous exchange of messages among multiple applications.

IBM WebSphere MQ implements the messaging handling services.

A number of queues are used by the IBM Intelligent Operations Center internally and also to receive external messages from other systems. Here are the main queues. Details about how these queues are used in the IBM Intelligent Operations Center can be found in Chapter 7, “Data flows” on page 189.

- ▶ Queues that are used to receive CAP messages from external systems:
 - IOC.CAP.IN
 - IOC_CAP_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY
- ▶ Queues that are used internally for processing KPIs:
 - IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY
 - IOC_KPI_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY
 - IOC_KPI_UPDATE_INTERNAL_USE_ONLY_DO_NOT_MODIFY
- ▶ Queues that are used internally by the business rules engine:
 - IOC_JRULES_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY
 - IOC_JRULES_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY
- ▶ Queues that are used internally for processing notifications:
 - IOC_NOTIFICATION_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY
 - IOC_NOTIFICATION_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY
- ▶ Queues that are used internally for processing resources:
 - IOC_RESOURCE_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY
 - IOC_RESOURCE_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY

IBM WebSphere Message Broker

IBM WebSphere Message Broker is a powerful information broker that allows business data, in the form of messages, to flow between disparate applications and across multiple hardware and software platforms. Rules can be applied to the data that is flowing through the WebSphere Message Broker to route, store, retrieve, and transform the information.

IBM WebSphere Message Broker implements the message bus services.

IBM Tivoli Netcool

In the IBM Intelligent Operations Center, the core event management process is performed by the IBM Tivoli Netcool® family of products. The main components of the IBM Tivoli Netcool family of products include IBM Tivoli Netcool/OMNibus and IBM Tivoli Netcool/Impact.

IBM Tivoli Netcool/OMNibus

IBM Tivoli Netcool/OMNibus implements the event handling services and is composed of the following two main components:

- ▶ **ObjectServer (NCOMS):** The ObjectServer is the database server at the core of IBM Tivoli Netcool/OMNibus. Event information is forwarded to the ObjectServer from external programs, such as probes, monitors, and gateways. The ObjectServer stores and manages this information in database tables and displays the information in the event list. The default name of the ObjectServer database is *NCOMS*.
- ▶ **Probes:** Probes connect to an event source, detect, and acquire event data, and forward the data to the ObjectServer as alerts. Probes use the logic that is specified in a rules file to manipulate the event elements before it converts them into the fields of an alert in the ObjectServer alerts.status table.

Each probe is uniquely designed to acquire event data from a specific source. Probes can acquire data from any stable data source, including devices, databases, and log files. The main probes and rule files that are used by the IBM Intelligent Operations Center are:

- CAP probe: The cap probe is an XML probe that uses the rules that are defined in the `xml_cap.rules` file to perform the initial processing of incoming CAP messages.
- Notification probe: The notification probe is an XML probe that uses the rules that are defined in the `xml_notification.rules` file to perform the initial processing of notification messages.
- Resource probe: The resources probe is an XML probe that uses the rules that are defined in the `xml_resource.rules` file to perform the initial processing of resource messages.

For more information about IBM Tivoli Netcool/OMNIBus, see *Certification Guide Series: IBM Tivoli Netcool/OMNIBus V7.2 Implementation*, SG24-7753.

IBM Tivoli Netcool/Impact

IBM Tivoli Netcool/Impact implements the event processing and enhancing services. It is composed mainly of the following components:

- ▶ IBM Tivoli Netcool/Impact server: This component manages the data model, services, and policies that make up an IBM Tivoli Netcool/Impact implementation. It runs the policies in real time in response to events that occur in the environment. Here are the main policies that are defined in the IBM Intelligent Operations Center. How these policies are used on each data flow is described in Chapter 7, “Data flows” on page 189.
 - IOC_Event_Main
 - IOC_Update_CAPDB
 - IOC_Event_Correlation
 - UTILS_LIBRARY_IOC_TSRM
 - IOC_Route_KPI_Event
 - IOC_Event_Notification
 - IOC_Event_Resource
- ▶ IBM Tivoli Netcool/OMNIBus Event Readers: These readers are services that monitor an IBM Tivoli Netcool/OMNIBus ObjectServer event source. When an event reader discovers a new, updated, or deleted alert in the ObjectServer, it retrieves the alert and sends it to an event queue. There it waits to be handled by an event processor, which then sends it to a policy engine for processing.

For more information about IBM Tivoli Netcool/Impact, see *Certification Guide Series: IBM Tivoli Netcool/Impact V4.0 Implementation*, SG24-7755.

IBM Sametime

The IBM Sametime component implements the instant messaging server.

IBM Lotus Domino

The IBM Lotus Domino component implements the contacts service.

IBM Tivoli Monitoring agents

The following monitoring agents are installed on the event server:

- ▶ IBM Tivoli Composite Application Manager Agent for WebSphere (also known as YN): This agent collects and forwards monitoring information about the performance of the application server to the Tivoli Enterprise Monitoring Server in the management server.

- ▶ IBM Tivoli Monitoring Agent for Linux OS (also known as LZ): This agent collects and forwards monitoring information about the performance of the Linux operating system to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring Agent for Web Servers (also known as HT): This agent collects and forwards monitoring information about the performance of the HTTP server to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring Agent for WebSphere MQ: This agent collects and forwards monitoring information about the performance of the messaging handling server to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring WebSphere MQ Configuration Agent (MC): This agent is used to monitor the WebSphere MQ configuration database.
- ▶ IBM Tivoli Monitoring for Lotus Sametime (S1): This agent collects and forwards monitoring information about the performance of the instant messaging server to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring for Lotus Domino (GB): This agent collects and forwards monitoring information about the performance of the contacts server to the Tivoli Enterprise Monitoring Server in the management server.

2.2.5 Topology of the data server

This section presents the detailed topology of the data server. Figure 2-6 shows an overview of the data server topology.

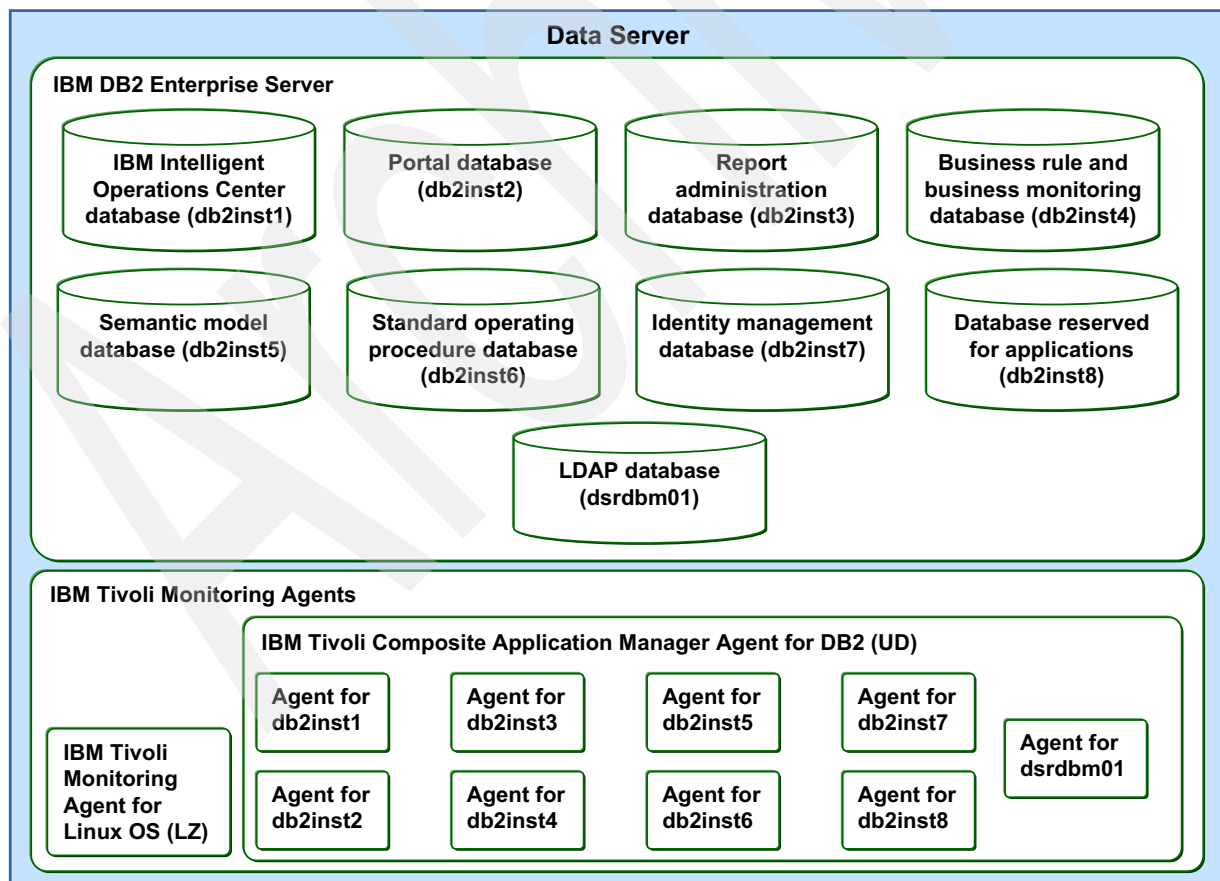


Figure 2-6 Topology of the data server

IBM DB2 Enterprise Server

IBM DB2 Enterprise Server provides the database infrastructure that is used by the IBM Intelligent Operations Center. The DB2 server supports multiple instances that can host multiple databases themselves.

Table 2-3 lists the database instances and databases that are initially installed on the IBM Intelligent Operations Center.

Table 2-3 Database instances and databases initially installed

Instance	Description	Database names
db2inst1	Main IBM Intelligent Operations Center database.	IOCDB. The IOCDB database contains two schemas, IOC and IOC.COMMON, which are relevant for administration of the IBM Intelligent Operations Center.
db2inst2	Portal databases.	<ul style="list-style-type: none"> ▶ CUSTDB. ▶ FDBKDB. ▶ LKMDDDB. ▶ JCRDB. ▶ COMMDB. ▶ RELDB.
db2inst3	Report administration databases.	<ul style="list-style-type: none"> ▶ CXLOGDB. ▶ CXCONTDB.
db2inst4	Registry, business rules, and business monitoring databases.	<ul style="list-style-type: none"> ▶ UDDIDB. ▶ WODMDCDB. ▶ MONITOR. ▶ WBMDB. ▶ RESDB.
db2inst5	Semantic model databases.	<ul style="list-style-type: none"> ▶ JTS. ▶ IIC.
db2inst6	Standard operating procedure administration database.	MAXIMO.
db2inst7	Identity management database.	TIMDB.
db2inst8	Not used. Reserved for internal applications.	
dsrdbm01	Directory LDAP databases.	<ul style="list-style-type: none"> ▶ LDAPDB. ▶ LDAPDB2B.

IBM Tivoli Monitoring agents

The following monitoring agents are installed on the data server:

- ▶ IBM Tivoli Monitoring Agent for Linux OS (also known as LZ): This agent collects and forwards monitoring information about the performance of the Linux operating system to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Composite Application Manager Agent for DB2 (also known as UD): This agent collects and forwards monitoring information about the performance of the database servers to the Tivoli Enterprise Monitoring Server on the management server. There is one agent for each database instance in this server:
 - db2inst1 agent
 - db2inst2 agent
 - db2inst3 agent
 - db2inst4 agent
 - db2inst5 agent

- db2inst6 agent
- db2inst7 agent
- db2inst8 agent
- dsrdbm01agent

2.2.6 Topology of the management server

This section presents the detailed topology of the management server. Figure 2-7 shows an overview of the management server topology.

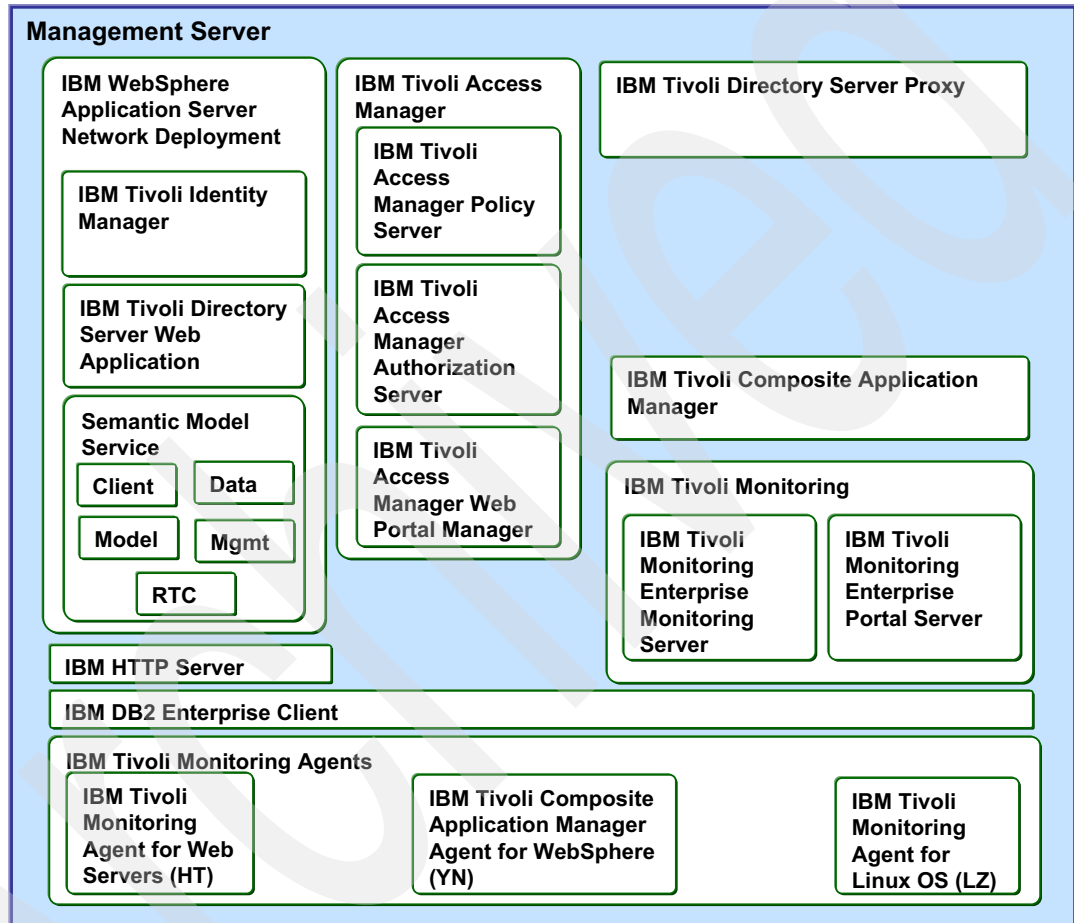


Figure 2-7 Topology of the management server

IBM WebSphere Application Server Network Deployment

The IBM WebSphere Application Server provides the runtime environment where the different components of the IBM Intelligent Operations Center are run. It uses a logical organization that is based on nodes and implements the management server service as described in 2.1.2, “Services overview” on page 26.

Note: A node is an administrative grouping of application servers for configuration and operational management within one operating system instance.

The IBM Intelligent Operations Center has several nodes that are initially configured on the management server. Table 2-4 lists these nodes, what application they run, and what service is being implemented.

Table 2-4 Nodes on the management server

Application server name	Node name	Application	Service implemented
IICCIsvcsServer1	IICCIsvcsNode1	Semantic model services	Semantic model service
IICDaAgSvcsServer1	IICDaAgSvcsNode1	Semantic model services	Semantic model service
IICMDLSvcsServer	IICMDLSvcsNode	Semantic model services	Semantic model service
IICMgmtSvcsServer1	IICMgmtSvcsNode1	Semantic model services	Semantic model service
IICRTCSvcsServer	IICRTCSvcsNode	Semantic model services	Semantic model service
tdsServer	tdsNode	IBM Tivoli Directory Server	Directory services
timServer	timNode	IBM Tivoli Identity Manager	Identity management services

IBM Tivoli Access Manager

IBM Tivoli Access Manager is a single sign-on (SSO) solution that authorizes and authenticates user access to web and other hosted applications. It is a scalable user authentication, authorization, and web SSO solution for enforcing security policies over a wide range of web and application resources. It centralizes user access management for online portal and business initiatives.

The following components of IBM Tivoli Access Manager are used by the IBM Intelligent Operations Center:

- ▶ IBM Tivoli Access Manager Policy Server
- ▶ IBM Tivoli Access Manager Authorization Server
- ▶ IBM Tivoli Access Manager Web Portal Manager

IBM Tivoli Composite Application Manager

IBM Tivoli Composite Application Manager, together with the IBM Tivoli Monitoring component, implement the system management service.

IBM Tivoli Composite Application Manager contains a managing server and some monitoring agents. The role of the agents is to collect and pass data that pertains to the application server performance, activity, workload, resource consumption, and overall health of the managing server. The role of the managing server is to provide the data repository, perform the bulk of the analysis, and serve as the user interface to observe and monitor the application servers. It also identifies whether there is a performance degradation of an application server or whether it becomes dysfunctional.

IBM Tivoli Monitoring

The IBM Tivoli Monitoring component, together with the IBM Tivoli Composite Application Manager component, implement the system management service.

IBM Tivoli Monitoring provides the monitoring infrastructure to ensure the IBM Intelligent Operations Center hardware and software environment is healthy and performing as expected. It contains the following two main components:

- ▶ IBM Tivoli Monitoring Enterprise Monitoring Server: Acts as a collection and control point for alerts that are received from agents and collects their performance and availability data.
- ▶ IBM Tivoli Monitoring Enterprise Portal Server: Is a repository for all graphical presentation of monitoring data. It provides the core presentation layer for the monitoring infrastructure, which allows for retrieval, manipulation, analysis, and reformatting of data.

IBM Tivoli Monitoring agents

The following monitoring agents are installed on the management server:

- ▶ IBM Tivoli Composite Application Manager Agent for WebSphere (also known as YN): This agent collects and forwards monitoring information about the performance of the application server to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring Agent for Linux OS (also known as LZ): This agent collects and forwards monitoring information about the performance of the Linux operating system to the Tivoli Enterprise Monitoring Server in the management server.
- ▶ IBM Tivoli Monitoring Agent for Web Servers (also known as HT): This agent collects and forwards monitoring information about the performance of the HTTP server to the Tivoli Enterprise Monitoring Server in the management server.

2.3 Hardware and software environment that is used in this publication

This section describes the hardware and software environment that is used during the development of this book. For the hardware and software requirements of the IBM Intelligent Operations Center, see the “Preparing for installation” topic in the IBM Intelligent Operations Center V1.5 Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/install_pre.html

As described in 2.1.1, “Servers overview” on page 24, the IBM Intelligent Operations Center solution is composed of five virtual servers:

- ▶ Application server
- ▶ Event server
- ▶ Database server
- ▶ Management server
- ▶ Installation server

The virtual machines are spread across one to many physical servers that depend on the capacity of the physical servers and the workload of the solution. For the test environment in this project, the IBM Intelligent Operations Center solution was deployed on an IBM BladeCenter® xH5, which included two physical servers, with two virtual machines on each server.

In preparation for the installation process, the BladeCenter xH5 was configured as follows:

- ▶ Three blade servers were used to deploy the five IBM Intelligent Operations Center servers (application server, data server, event server, management server, and install server).

- ▶ Three storage pools (SPs) (RAID 10) were created using IBM Storage Configuration Manager:
 - SP1: 7 TB
 - SP2: 2 TB
 - SP3: 300 GB

The storage pools were allocated to each blade server.

- ▶ A virtualized environment was set up using VMware ESXi V4 no cost license. Five virtual machines (VMs), one for each IBM Intelligent Operations Center server, were created on the three blade servers.

Virtual machines: Both VMWare and Keyboard, Video and Mouse (KVM) hypervisors are supported. The virtual machine creation is the job of the IBM Intelligent Operations Center solution installers. They create virtual machines with a base RHEL configuration, then install those virtual machines from the installation server and scripts. KVM provides a lower-cost alternative.

- ▶ The five virtual machines were configured on a private network and intercommunicated across the physical servers on that private subnet. The BladeCenter required five external IP addresses to be remotely administered: One IP address for the Advanced Management Module (AMM), and four for the SANs storage and RAID adapters. The configuration also needed two additional external IP addresses for the hypervisor hosts running on the two physical servers. These IP addresses bridged the virtual servers to the Internet.

Table 2-5 shows the BladeCenter resources that were used in our test environment.

Table 2-5 Hardware resources that were used in this project

Blade server	Real memory	Physical processor (# of cores)	Storage pool
Blade 1 Model Hx5 - 7872AC1	64 GB	8	SP1 1.3 TB
Blade 2 Model Hx5 - 7872AC1	64 GB	8	SP2 1.4 TB
Blade 3 Model HS22 - 7870AC1	16 GB	8	N/A

Table 2-6 shows the IBM Intelligent Operations Center servers and the VMs where they were deployed in our test environment.

Table 2-6 IBM Intelligent Operations Center execution environment for this project

IBM Intelligent Operations Center server	Host name	Blade server	VM name	vCPU	vMemory	Initial disk size	Final disk size (after installation)
Application server	ioc-icp004.itso.ibm.com	2	ioc-icp004	4	24 GB	308 GB	208 GB
Data server	ioc-icp002.itso.ibm.com	1	ioc-icp002	4	16 GB	308 GB	208 GB
Event server	ioc-icp003.itso.ibm.com	2	ioc-icp003	4	16 GB	308 GB	208 GB
Management server	ioc-icp001.itso.ibm.com	1	ioc-icp001	4	16 GB	308 GB	208 GB
Install server	ioc-icp000.itso.ibm.com	3	ioc-icp000	2	4 GB	250 GB	250 GB

Administration fundamentals

This chapter describes the basic tools available to IBM Intelligent Operations Center administrators to perform daily operations and diagnose problems.

Topics that are covered in this chapter include:

- ▶ Platform control tool (IOControl or PCT)
- ▶ System Verification Check
- ▶ Administration Consoles
- ▶ Sample Event Publisher portlet
- ▶ System monitoring
- ▶ WebSphere MQ Explorer
- ▶ Database control center
- ▶ IBM Tivoli Netcool/OMNIBus database utility
- ▶ MustGather tool
- ▶ System-wide configuration properties
- ▶ Solution logs
- ▶ Checking the health of the solution

For information about procedures for the regular maintenance of this solution, see Chapter 4, “Preventive maintenance” on page 83.

For detailed information and examples about problem diagnostic tests and resolution, see Chapter 6, “Troubleshooting” on page 137.

3.1 Platform control tool (IOControl or PCT)

IBM Intelligent Operations Center includes the **IOControl** command to start, stop, and query the status of the servers. The **IOControl.sh** script is on the management server in the following directory:

```
/opt/IBM/ISP/mgmt/scripts
```

Tip: The **IOControl.sh** command must be run as the **ibmadmin** user. If you are not logged on as **ibmadmin**, run **su - ibmadmin** to switch to the **ibmadmin** user.

The **IOControl** command can be run for all or individual servers. The **start** command ensures that the underlining services are started in the correct sequence.

Status command: After successful installation of the IBM Intelligent Operations Center product, run the following status command to verify that all the IBM Intelligent Operations Center services are installed and functioning:

```
cd /opt/IBM/ISP/mgmt/scripts
./IOControl.sh status all <password>
```

The syntax of the **IOControl** command is:

```
IOControl.sh <Action> <Target> <password>
```

Where:

- ▶ Action can be start, stop, status, or help.
- ▶ Target is either all or an individual server name.
- ▶ Password is the password for the Platform Control Tool that is defined when the solution was deployed.

To see the options available for **IOControl**, run the following command:

```
cd /opt/IBM/ISP/mgmt/scripts
./IOControl.sh help <password>
```

Figure 3-1 shows the results. Notice the various target server names.

```
[ibmadmin@ioc-icp001 root]$ /opt/IBM/ISP/mgmt/scripts/IOControl.sh help <password>
Sun Jul 15 19:58:37 EDT 2012
Usage: IOControl.sh <action> <target> <password>
Action options:
  start      -      Start server(s)
  stop      -      Stop server(s)
  status    -      Check server status
  help      -      Get help message
Target options:
  all       -      All platform servers
  db24po    -      IBM DB2 Enterprise server for Portal Server
  db24wbm   -      IBM DB2 Enterprise server for WebSphere Business Monitor
  db24sol   -      IBM DB2 Enterprise server for Solution
  db24ana   -      IBM DB2 Enterprise server for Analytics Server
  db24mgmt  -      IBM DB2 Enterprise server for Management Server
  db24tsrm  -      IBM DB2 Enterprise server for TSRM Server
  db24sms   -      IBM DB2 Enterprise server for Semantic Model Services
  tds       -      IBM Tivoli Directory Server
  tdspxyapp -      IBM Tivoli Directory Server Proxy (Application Server)
  tdspxyevt -      IBM Tivoli Directory Server Proxy (Event Server)
  tdspxymgt -      IBM Tivoli Directory Server Proxy (Management Server)
  tdsappsrv -      IBM Tivoli Directory Server Application Server
  tamps     -      IBM Tivoli Access Manager Policy Server
  tamas     -      IBM Tivoli Access Manager Authorization Server
  tamwpm    -      IBM Tivoli Access Manager Web Portal Manager
  tamweb    -      IBM Tivoli Access Manager WebSEAL
  tems      -      IBM Tivoli Monitoring Enterprise Monitoring Server
  teps      -      IBM Tivoli Monitoring Enterprise Portal Server
  tim       -      IBM Tivoli Identity Manager
  appdmgr   -      IBM WebSphere Application Server Deployment Manager
  cplex     -      IBM WebSphere Application Server for CPLEX
  ihs       -      IBM HTTP Server for Runtime (Application Server)
  ihsevt    -      IBM HTTP Server for Runtime (Event Server)
  ihsmgmt   -      IBM HTTP Server for Runtime (Management Server)
  ncob      -      IBM Tivoli Netcool OMNIBus
  nci       -      IBM Tivoli Netcool Impact
  wbm       -      IBM WebSphere Business Monitor
  st        -      IBM Lotus Sametime
  stpxy     -      IBM Lotus Sametime Proxy Application Server
  wpe       -      IBM WebSphere Portal Extend
  wmb       -      IBM WebSphere Message Broker
  cognos    -      IBM Cognos Business Intelligence
  tsrm      -      IBM Tivoli Service Request Manager
  wodm      -      IBM WebSphere Operations Decision Manager
  wodmdc    -      IBM WebSphere Operations Decision Manager (Decision Center)
  smsclt    -      IBM Semantic Model Services (Client Services)
  smsdaaq   -      IBM Semantic Model Services (Data Services)
  smsmdl    -      IBM Semantic Model Services (Model Services)
  smsmgmt   -      IBM Semantic Model Services (Mgmt. Services)
  smsrtc    -      IBM Semantic Model Services (RTC Services)
  iocxml    -      IBM Intelligent Operations Center XML probe
```

Figure 3-1 IOControl command actions and target options

3.1.1 Starting servers with IOControl

There are two options to start the servers with `IOControl.sh`:

- ▶ Start all servers.

To start all the IBM Intelligent Operations Center servers, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts/  
./IOControl.sh start all <password>
```

Time to start the servers: It takes about 30 minutes to start all the servers.

- ▶ Start individual servers.

To start an individual server, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts  
./IOControl.sh start <Target> <password>
```

For example, to start the business monitoring service, run the following command:

```
./IOControl.sh start wbm <password>
```

3.1.2 Stopping servers with IOControl

There are two options to stop the servers with the `IOControl.sh` command.

- ▶ Stop all servers.

To stop all the IBM Intelligent Operations Center servers, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts  
./IOControl.sh stop all <password>
```

- ▶ Stop individual servers.

To stop an individual server, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts  
./IOControl.sh stop <Target> <password>
```

For example, to stop the message bus service, run the following command:

```
./IOControl.sh stop wmb <password>
```

Figure 3-2 shows the results of the stop message bus service command. Note that *wbm* is the business monitoring service or IBM Business Monitor and *wmb* is the message bus service or IBM WebSphere Message Broker.

```
Executing query command...completed.  
IBM WebSphere Message Broker [ off ]  
Command completed successfully.
```

Figure 3-2 Stopping the message bus service with IOControl

Important: When you stop all the servers, ensure that the servers are fully stopped by using the `status` option before you restart them. Many times the prompt comes back on the console but the background process is still running to stop all the servers.

3.1.3 Querying the server status with IOControl

There are two options to determine the status of the IBM Intelligent Operations Center servers with IOControl:

- ▶ Status of all the servers.

To check the status of all the IBM Intelligent Operations Center servers, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts  
./IOControl.sh status all <password>
```

- ▶ Status of individual servers.

To check the status of an individual server, run the following command on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts  
./IOControl.sh status <Target> <password>
```

For example, run the following command to check the status of the message bus:

```
./IOControl.sh status wmb <password>
```

Querying the status of all the servers displays the output that is shown in Figure 3-3.

```
[root@icp001 scripts]# ./IOControl.sh status all <admin password>
Executing query command .....completed.
IBM DB2 Enterprise server for Portal Server [ on ]
IBM DB2 Enterprise server for WebSphere Business Monitor [ on ]
IBM DB2 Enterprise server for Solution [ on ]
IBM DB2 Enterprise server for Analytics Server [ on ]
IBM DB2 Enterprise server for Management Server [ on ]
IBM DB2 Enterprise server for TSRM Server [ on ]
IBM DB2 Enterprise server for IIC (Model Manager) [ on ]
IBM Tivoli Directory Server [ on ]
IBM Tivoli Directory Server Proxy (Application Server) [ on ]
IBM Tivoli Directory Server Proxy (Event Server) [ on ]
IBM Tivoli Directory Server Proxy (Management Server) [ on ]
IBM Tivoli Directory Server Application Server [ on ]
IBM Tivoli Access Manager Policy Server [ on ]
IBM Tivoli Access Manager Authorization Server [ on ]
IBM Tivoli Access Manager Web Portal Manager [ on ]
IBM Tivoli Access Manager WebSEAL [ on ]
IBM WebSphere Message Broker [ on ]
IBM WebSphere Application Server Deployment Manager [ on ]
IBM WebSphere Business Monitor [ on ]
IBM WebSphere Operations Decision Manager [ on ]
IBM Tivoli Identity Manager [ on ]
IBM HTTP Server (Application Server) [ on ]
IBM HTTP Server (Event Server) [ on ]
IBM HTTP Server (Management) [ on ]
IBM WebSphere Application Server for CPLEX [ on ]
IBM Tivoli Netcool OMNIBus [ on ]
IBM Tivoli Netcool Impact [ on ]
IBM Lotus Sametime [ on ]
IBM Lotus Sametime Proxy Application Server [ on ]
IBM COGNOS Business Intelligence [ on ]
IBM WebSphere Portal Extend [ on ]
IBM Tivoli Service Request Manager [ on ]
IBM Tivoli Monitoring Enterprise Monitoring Server [ on ]
IBM Tivoli Monitoring Enterprise Portal Server [ on ]
IBM Integrated Information Core (Client Services) [ on ]
IBM Integrated Information Core (Data Services) [ on ]
IBM Integrated Information Core (Model Services) [ on ]
IBM Integrated Information Core (RTC Services) [ on ]
Command completed successfully.
```

Figure 3-3 Querying the status of all the IBM Intelligent Operations Center servers

3.2 System Verification Check

System Verification Check is a portlet-based, easy to use tool that IBM Intelligent Operations Center administrators can use to run most of the tests that are needed to determine the health of the overall system and individual components.

There are several scenarios where it is helpful to use the System Verification Check tool. For example:

- ▶ Immediately after you install IBM Intelligent Operations Center to verify that all the services and end-to-end flows are working properly
- ▶ After you stop servers, reboot systems, and restart servers to verify that all services are restarted and everything is back up and running
- ▶ When you perform problem determination procedures and you must find the failing component

To access the System Verification Check tool, complete the following steps:

1. Log in to the IBM Intelligent Operations Center.
2. On the left navigation frame, expand **Intelligent Operations** → **Administration Tools**.
3. Click **System Verification Check**. The System Verification Check page opens (Figure 3-4).

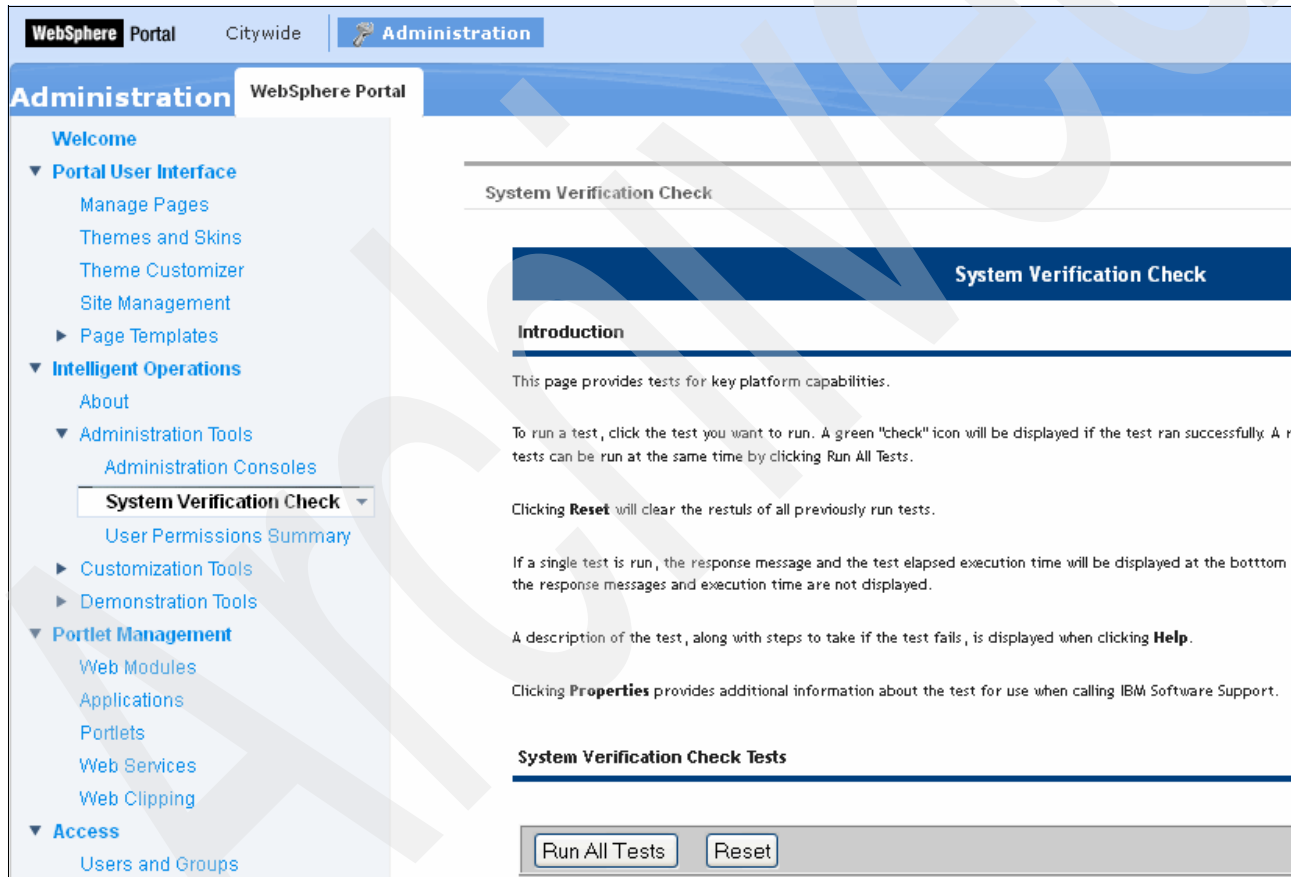


Figure 3-4 System Verification Check page

3.2.1 Running System Verification Check tests

Each test in the System Verification Check has a button with the name of the test and the server or components it tests. Figure 3-5 on page 50, Figure 3-6 on page 51, and Figure 3-7 on page 51 show of all the available System Verification Check tests.

To run a test, click the button for the test you want to run.

Help includes the following information:

- ▶ Description of the test.
- ▶ Resources tested.
- ▶ Problem determination procedures that the administrator must follow if the test fails, including logs to check, location of the logs, commands to run, and so on.

System Verification Check Tests		
<input type="button" value="Run All Tests"/> <input type="button" value="Reset"/>		
Test	Result	Troubleshooting
<input type="button" value="IOC Event Flow"/>		Help + Properties
<input type="button" value="IOC Notification Flow"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Directory Server - Application)"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Directory Server - Data)"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Directory Server - Event)"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Directory Server - Management)"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Identity Manager API)"/>		Help + Properties
<input type="button" value="Account Management (Tivoli Identity Manager Console)"/>		Help + Properties
<input type="button" value="Analytics (Cognos Gateway Console)"/>		Help + Properties
<input type="button" value="Application Server (WebSphere Application Server Web Service)"/>		Help + Properties
<input type="button" value="Business Rules (WebSphere Operational Decision Manager JRules Console)"/>		Help + Properties
<input type="button" value="Business Rules (WebSphere Operational Decision Manager JRules Rule)"/>		Help + Properties
<input type="button" value="Collaboration (Lotus Domino Console)"/>		Help + Properties
<input type="button" value="Collaboration (Lotus Sametime Console)"/>		Help + Properties
<input type="button" value="Collaboration (Lotus Sametime Proxy Console)"/>		Help + Properties
<input type="button" value="Database (DB2 Instance - db2inst1)"/>		Help + Properties
<input type="button" value="Database (DB2 Instance - db2inst2)"/>		Help + Properties
<input type="button" value="Database (DB2 Instance - db2inst3)"/>		Help + Properties

Figure 3-5 Available System Verification Check tests (1 of 3)

Database (DB2 Instance - db2inst4)	Help		+ Properties
Database (DB2 Instance - db2inst5)	Help		+ Properties
Database (DB2 Instance - db2inst6)	Help		+ Properties
Database (DB2 Instance - db2inst7)	Help		+ Properties
Database (DB2 Instance - db2inst8)	Help		+ Properties
Database (DB2 Instance - dsrdbm01)	Help		+ Properties
Database (DB2)	Help		+ Properties
Directory (UDDI V3 HTTPS)	Help		+ Properties
Directory (UDDI V3)	Help		+ Properties
Internal Diagnostic (Echo REST remoted)	Help		+ Properties
Messaging (WebSphere Message Broker Publish/Subscribe topic)	Help		+ Properties
Messaging (WebSphere Message Broker/Queue install check)	Help		+ Properties
Messaging (WebSphere Message Broker/Queue queue)	Help		+ Properties
Messaging (WebSphere Message Queue Publish/Subscribe topic)	Help		+ Properties
Monitoring (Netcool Impact Console)	Help		+ Properties
Monitoring (Netcool Omnibus)	Help		+ Properties



Figure 3-6 Available System Verification Check tests (2 of 3)

Monitoring (Tivoli Composite Application Manager Agents - Application)	Help		+ Properties
Monitoring (Tivoli Composite Application Manager Agents - DB2 instances)	Help		+ Properties
Monitoring (Tivoli Composite Application Manager Agents - Data)	Help		+ Properties
Monitoring (Tivoli Composite Application Manager Agents - Event)	Help		+ Properties
Monitoring (Tivoli Composite Application Manager Agents - Management)	Help		+ Properties
Monitoring (Tivoli Enterprise Monitoring Server)	Help		+ Properties
Monitoring (WebSphere Business Monitor Business Space Console)	Help		+ Properties
Monitoring (WebSphere Business Monitor Mobile Device Console)	Help		+ Properties
Policy (Tivoli Service Request Manager Maximo Console)	Help		+ Properties
Security (Tivoli Access Manager Web Portal Manager)	Help		+ Properties
Security (Tivoli Access Manager)	Help		+ Properties
Security (WebSEAL Console)	Help		+ Properties
Web Server (IBM HTTP Server Console)	Help		+ Properties

Figure 3-7 Available System Verification Check tests (3 of 3)

The special System Verification Check tests are:

- Run All Tests** Runs all tests sequentially.
- IOC Event Flow** Tests the full event flow that is described in 7.1, “Event flow” on page 190. This test verifies that the critical components of the IBM Intelligent Operations Center event processing system are working as expected. It sends a message to the IOC.CAP.IN queue. The message follows the event flow and, if the test is successful, returns a green check mark. The test event is not displayed in the IBM Intelligent Operations Center graphical user interface (GUI).
- IOC Notification Flow** Tests the full notification flow that is described in 7.4, “Notification flow” on page 206. This test verifies that the critical components of the IBM Intelligent Operations Center notification processing system are working as expected. It sends a message to the IOC.NOTIFICATION.IN queue. The message follows the notification flow and, if the test is successful, it returns a green check mark. The test notification is not displayed in the IBM Intelligent Operations Center GUI.

After the test runs, an icon appears in the Result column. A green check icon  is displayed when the test completes successfully. A red X icon  is displayed when the test fails.

If a test fails, follow the problem determination instructions for the test to resolve the errors. These instructions can be accessed by clicking the red x icon or the **Help** link. For details, see 3.2.2, “Performing problem determination procedures” on page 52.

Tip: IOC Event Flow and IOC Notification Flow tests are time sensitive and might report a false fail result. If these tests fail, run them for a second time to make sure that the test is really failing.

3.2.2 Performing problem determination procedures

If the System Verification Check test fails, perform the problem determination procedures that are documented in the Help link for the test.

Figure 3-8 shows a situation where the IOC Event Flow test failed.

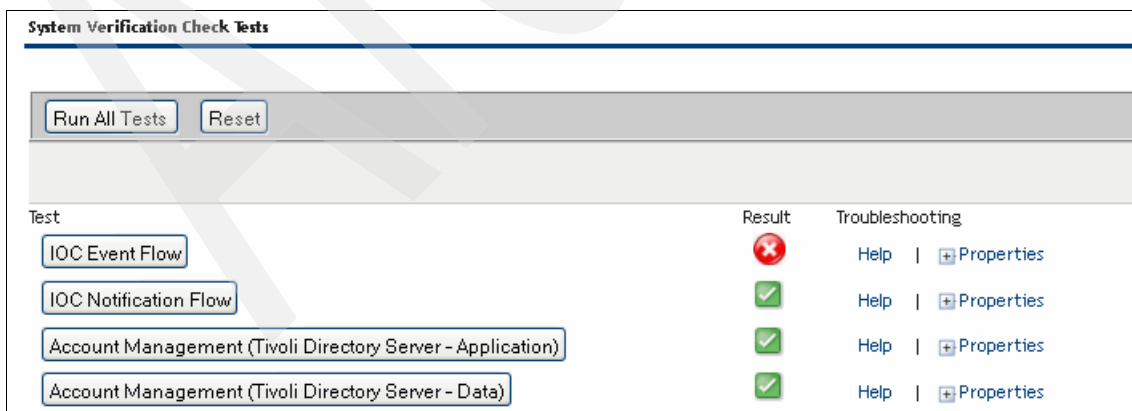


Figure 3-8 IOC event flow test failed

Clicking the red X icon or the **Help** link displays the IBM Intelligent Operations Center online help, which includes the problem determination procedure that the administrator must perform next. Figure 3-9 shows the problem determination procedure to follow when the IOC Event Flow test fails.

Problem determination

If the Intelligent Operation Center Event Flow test fails, do the following to find and resolve the access problem.

Procedure

1. Check that the IBM Intelligent Operations Center components are running.
 - a. In a command window on the event server, run `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password` Intelligent Operations Center administrator password defined when the IBM Intelligent Operations Center was deployed.
 - b. If there are components that are not running, start those components by running `/opt/IBM/ISP/mgmt/scripts/IOControl.sh start password component_ID` where `password` is the IBM Intelligent Operations Center administrator password defined when the IBM Intelligent Operations Center was deployed and `component_ID` is an ID listed under Target Options when running `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password`.
2. Start the Tivoli Netcool/OMNIBus probe by running the following on the event server.

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/props/ioc_xml.props &
```
3. Review the Netcool/OMNIBus log (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) on the event server for any errors.

What to do next

Resolve any issues or errors found and retry the test.

Figure 3-9 Problem determination procedure for IOC Event Flow failure

Complete the steps that are documented in the procedure that is shown in Figure 3-9:

1. Check that the IBM Intelligent Operations Center components are running. In a command window on the management server, run the following command:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all <password>
```

Figure 3-10 shows the results of the **status** command.

```
ibmadmin@ioc-icp001:/opt/IBM/ISP/mgmt/scripts
File Edit View Terminal Tabs Help
IBM DB2 Enterprise server for Semantic Model Services [ on ]
IBM Tivoli Directory Server [ on ]
IBM Tivoli Directory Server Proxy (Application Server) [ on ]
IBM Tivoli Directory Server Proxy (Event Server) [ on ]
IBM Tivoli Directory Server Proxy (Management Server) [ on ]
IBM Tivoli Directory Server Application Server [ on ]
IBM Tivoli Access Manager Policy Server [ on ]
IBM Tivoli Access Manager Authorization Server [ on ]
IBM Tivoli Access Manager Web Portal Manager [ on ]
IBM Tivoli Access Manager WebSEAL [ on ]
IBM WebSphere Message Broker [ on ]
IBM WebSphere Application Server Deployment Manager [ on ]
IBM WebSphere Business Monitor [ on ]
IBM WebSphere Operations Decision Manager [ on ]
IBM WebSphere Operations Decision Manager (Decision Center) [ on ]
IBM Tivoli Identity Manager [ on ]
IBM HTTP Server (Application Server) [ on ]
IBM HTTP Server (Event Server) [ on ]
IBM HTTP Server (Management Server) [ on ]
IBM WebSphere Application Server for CPLEX [ on ]
IBM Tivoli Netcool OMNIBus [ on ]
IBM Tivoli Netcool Impact [ off ]
IBM Lotus Sametime [ on ]
IBM Lotus Sametime Proxy Application Server [ on ]
IBM COGNOS Business Intelligence [ on ]
IBM WebSphere Portal Extend [ on ]
IBM Tivoli Service Request Manager [ on ]
IBM Tivoli Monitoring Enterprise Monitoring Server [ on ]
IBM Tivoli Monitoring Enterprise Portal Server [ on ]
IBM Semantic Model Services (Client Services) [ on ]
IBM Semantic Model Services (Data Services) [ on ]
IBM Semantic Model Services (Model Services) [ on ]
IBM Semantic Model Services (Management Services) [ on ]
IBM Semantic Model Services (RTC Services) [ on ]
Intelligent Operations Center XML Probe [ on ]
Command completed successfully.
```

Figure 3-10 IBM Tivoli Netcool/Impact status off

2. Start the components that are not running. In this example, start IBM Tivoli Netcool/Impact. Figure 3-1 on page 45 shows that the target to start IBM Tivoli Netcool/Impact is *nci*.

In a command window on the management server, run the following command:

```
cd /opt/IBM/ISP/mgmt/scripts
./IOCControl.sh start nci <password>
```

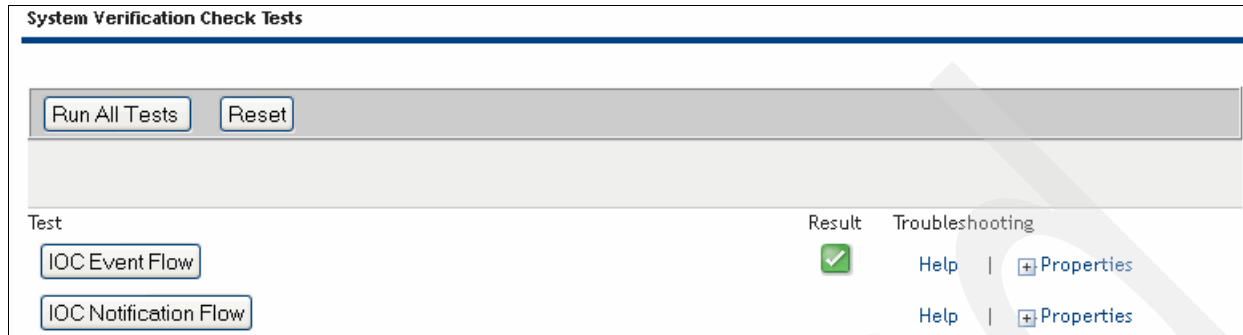
Figure 3-11 shows the results of the **start** command.

```
Tue Jul 17 00:04:42 EDT 2012
[ibmadmin@ioc-icp001 root]$ /opt/IBM/ISP/mgmt/scripts/IOCControl.sh start nci password
Tue Jul 17 00:06:00 EDT 2012

Executing start command.....completed.
Executing query command.....completed.
  IBM Tivoli Netcool Impact [ on ]
Command completed successfully.
```

Figure 3-11 IBM Tivoli Netcool/Impact started

3. Reset the System Verification Check test results. Click **Reset** to clear the previous test results.
4. Run the IOC Event Flow test again. Figure 3-12 shows the successful test results.



The screenshot displays the 'System Verification Check Tests' interface. At the top, there are two buttons: 'Run All Tests' and 'Reset'. Below this, a table lists the test results. The 'IOC Event Flow' test is marked as successful with a green checkmark, and the 'IOC Notification Flow' test is also marked as successful with a green checkmark. Each test entry includes a 'Help' link and a '+ Properties' link.

Test	Result	Troubleshooting
IOC Event Flow	✓	Help + Properties
IOC Notification Flow	✓	Help + Properties

Figure 3-12 IOC Event Flow test successful

3.3 Administration Consoles

Administration Consoles is a portlet in the IBM Intelligent Operations Center that brings together the web-based administration consoles for several servers of the solution. Use this portlet to access the administration console for a particular component. Chapter 6, “Troubleshooting” on page 137 shows how to use a specific administration console in the troubleshooting scenarios.

To access Administration Consoles, complete the following steps:

1. Log in to IBM Intelligent Operations Center.
2. On the left navigation frame, expand **Intelligent Operations** → **Administration Tools**.

3. Click **Administration Consoles**. The page opens, as shown in Figure 3-13.

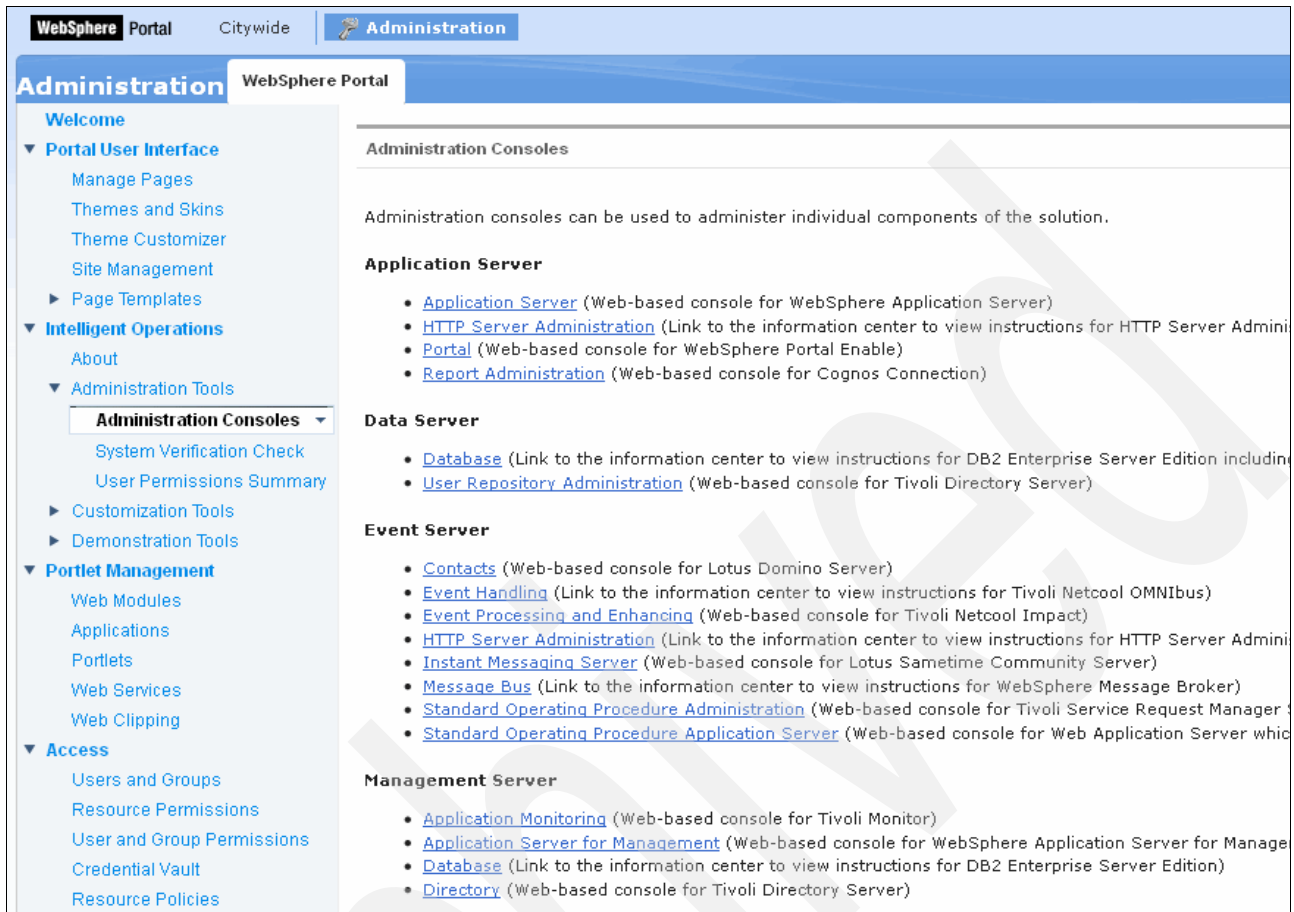


Figure 3-13 IBM Intelligent Operations Center Administration Consoles

You can administer various services from this page. Table 3-1 is a list of the web-based administration consoles that can be started from the Administration Consoles portlet.

Table 3-1 Web-based administration consoles

Console	Description
Application Server	
Application Server	Web-based console for IBM WebSphere Application Server. Use this console to administer various services that are provided by IBM Intelligent Operations Center. You can control the servers, manage resources and service providers, and change host and other environmental settings.
Report Administration	Web-based console for IBM Cognos Connection. Use this console to set up reports. You can create reports or modify existing ones. You can also configure data sources, set up public and private folders, define permissions and distribution, and schedule reports to run automatically.
Data Server	
Database	This is a link to the Information Center to view instructions about DB2 Enterprise Server Edition administration, including DB2 Spatial Extender. You can perform tasks with the database control center GUI or the command line.

Console	Description
Event Server	
Contacts	Web-based console for Lotus Domino Server. Use this console to view current settings in the names.nsf database. Names.nsf is used to configure Lotus Domino Server. Configuration changes can be made with the Domino Administration client.
Contacts Administration	This is a link to the Information Center to view instructions for the Domino Administration client. For details about how to download and set up Domino Administration client for Lotus Domino contacts administration, use the link to Information Center.
Event Handling	This is a link to the Information Center to view instructions for IBM Tivoli Netcool/OMNIBus. To administer event handling with the object server GUI, use Tivoli Netcool/OMNIBus (see 3.8, "IBM Tivoli Netcool/OMNIBus database utility" on page 76).
Event Processing and Enhancing	Web-based console for Tivoli Netcool/Impact. Use this console to administer event processing. For example, you can check database connections, data source connections, event process initiation, policy status, and logs.
Instant Messaging Server	Web-based console for Lotus Sametime Community Server. Use this console to administer instant messaging.
Message Bus	This is a link to the Information Center for IBM WebSphere Message Broker. You can find information about how to check the message status with WebSphere Message Broker.
Standard Operating Procedure Administration	Web-based console for Tivoli Service Request Manager Start Center. Use this console to define resources and SOPs. You can define available resources and activities for event management in the IBM Intelligent Operations Center.
Standard Operating Procedure Application Server	Web-based console for WebSphere Application Server, which serves Tivoli Service Request Manager.
Management Server	
Application Monitoring	Web-based console for Tivoli Monitoring. Use this console to administer application monitoring. You can work with this console for system health checks (see 3.5, "System monitoring" on page 65).
Application Server for Management	Web-based console for WebSphere Application Server for Management, including Tivoli Access Manager and WebSEAL. Use this console to administer integrated applications. This administration includes security administration with Tivoli Access Manager and WebSEAL.
Database	This is a link to the Information Center. For details about how to administer the database with DB2 Enterprise Server Edition, use the link to the Information Center. You can perform tasks with the database control center GUI or the command line.
Directory	Web-based console for Tivoli Directory Server. Use this console to administer the user's directory.

Table 3-2 shows the administrator user ID for each administration console that is listed in the Administration Consoles page. The corresponding passwords are set during the IBM Intelligent Operations Center installation process and is the topology password.

Table 3-2 IBM Intelligent Operations Center servers administrator's user IDs

Administration console	Administrator user ID	Comments
Application Server	waswebadmin	
Portal	wpsadmin	Single Sign-On is configured during installation. The user ID and password are not needed to access the console.
Report Administration	wpsadmin	Single Sign-On is configured during installation. The user ID and password are not needed to access the console if you are logged in as wpsadmin.
User Repository	cn=root	
Contacts	notes admin	
Event Processing and Enhancing	admin	The password is different from the default password of other services accounts.
Instant Messaging	notes admin	
Standard Operating Procedure Administration	maxadmin	
Standard Operating Procedure Application Server	waswebadmin	
Application Monitoring and system monitoring	sysadmin	
Application Server for Management	waswebadmin	
Directory	cn=root	The LDAP administrator must configure the cn=root account. For the first login, use user ID=superadmin and password=secret.

Figure 3-14 shows, as an example, the web-based Application Server administration console that is called *Integrated Solutions Console* being started from the Administration Consoles portlet.

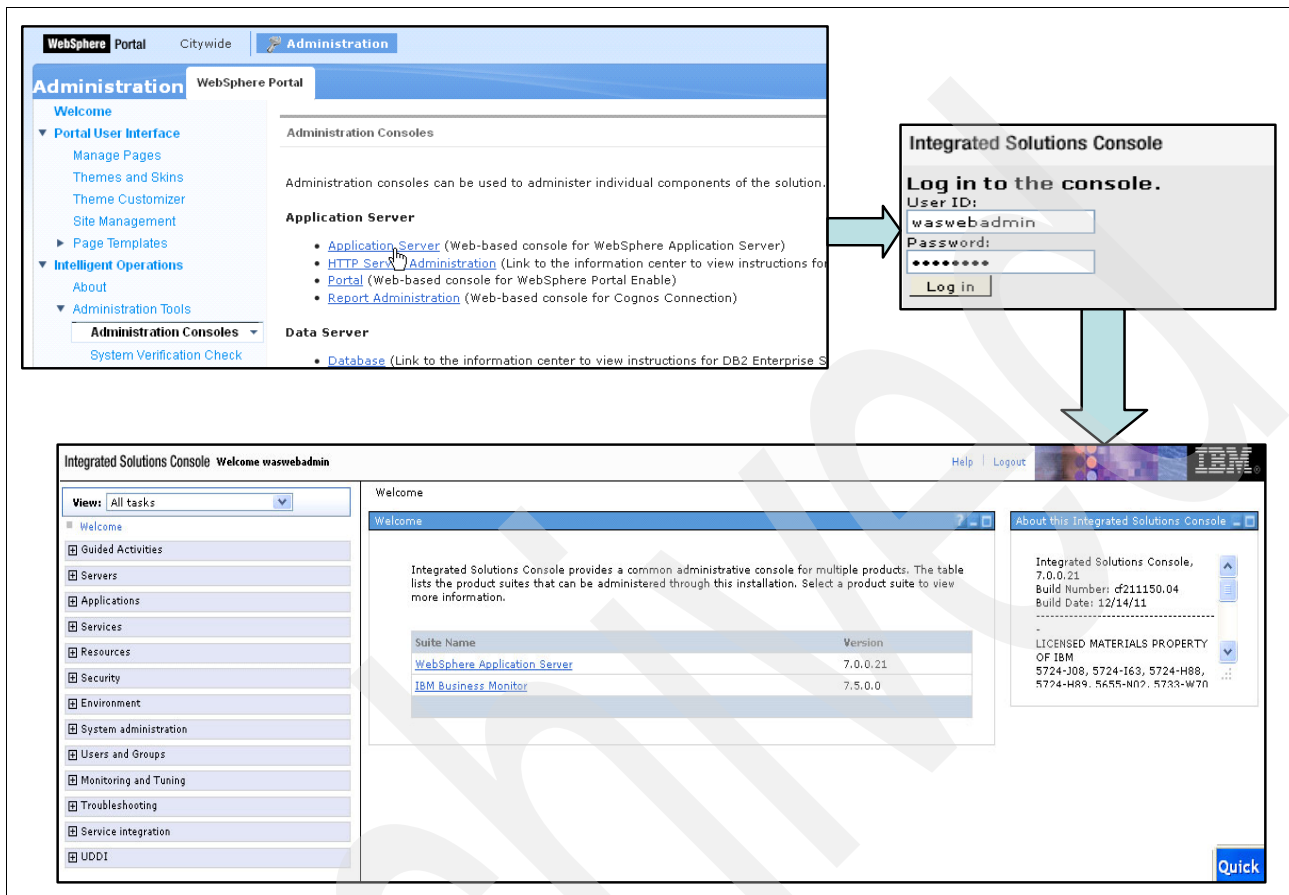


Figure 3-14 Starting the Application Server web-based administration console

3.4 Sample Event Publisher portlet

The *Sample Event Publisher* portlet is an automated test tool that is intended for an administrator managing or verifying the solution. An administrator can use the Sample Event Publisher portlet as a client application to test the publication of events, KPI, and notification messages in the IBM Intelligent Operations Center.

For more information about the usage and customization of the Sample Event Publisher portlet, see the “Sample Publisher” topic in the IBM Intelligent Operations Center V1.5 Information Center at:

<http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/SamplePublisherPortletHelp.html>

3.4.1 Creating test events

This section demonstrates how to use the Sample Event Publisher portlet to generate a test CAP event. Complete the following steps:

1. Start the Sample Event Publisher portlet. In the IBM Intelligent Operations Center, in the left pane, click **Intelligent Operations** → **Demonstration Tools** → **Sample Event Publisher** (Figure 3-15).



Figure 3-15 Starting the Sample Event Publisher portlet

2. On the Event CAP tab, you can select a pre-canned CAP event or KPI to test the corresponding flows. You can edit the XML in the form as needed.
 - a. To test the CAP event, submit the form that is shown in Figure 3-16. Notice that the `<code>` element value is *Event*.

A screenshot of the 'Sample Event Publisher' portlet interface. The interface has three tabs: 'Event CAP', 'Event Form', and 'Notification'. The 'Event CAP' tab is active. Below the tabs, there is a text prompt: 'Select a sample CAP event to view, modify, and publish into the Operations Center.' There are three dropdown menus: 'Category' with 'Fire' selected, 'Sample Event' with 'Large Wildfire' selected, and 'Event Message' with a text area containing XML code. The XML code is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>a06f5f40-a948-41b2-a6a4-163c785ca2e8</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T16:04:05-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <restriction/>
  <code>Event</code>
  <info>
    <language>en_US</language>
    <category>Fire</category>
    <event>Large Wildfire</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <headline>Large Wildfire moving Rapidly West - Test event</headline>
    <description>Approx 40 acres of unpopulated land burning. Fires
moving rapidly east toward populated areas.</description>
    <area>
      <areaDesc>West of I-75 close to Chapel Trail Nature Preserve.
</areaDesc>
      <circle>26.02069,-80.59879 0</circle>
    </area>
  </info>
</alert>
```

The XML code is displayed in a text area with a light blue border. Two lines of the XML code are highlighted with red boxes: the line containing `<code>Event</code>` and the line containing `<headline>Large Wildfire moving Rapidly West - Test event</headline>`.

Figure 3-16 Test CAP event with Sample Event Publisher portlet

- b. Select **Randomized Events** (Figure 3-17) to ensure that the identifier is unique. Click **Submit Event**.

Event Instance Count: 1
 Randomize Events:
 Submit Event

Figure 3-17 Sample Event Publisher portlet - Randomized Events

3. Verify that the event is displayed in the IBM Intelligent Operations Center GUI:
 - a. Click **Citywide** → **Supervisor: Operations**.
 - b. The test event should be displayed in the **Details** → **Events and Incidents** tab (Figure 3-18).

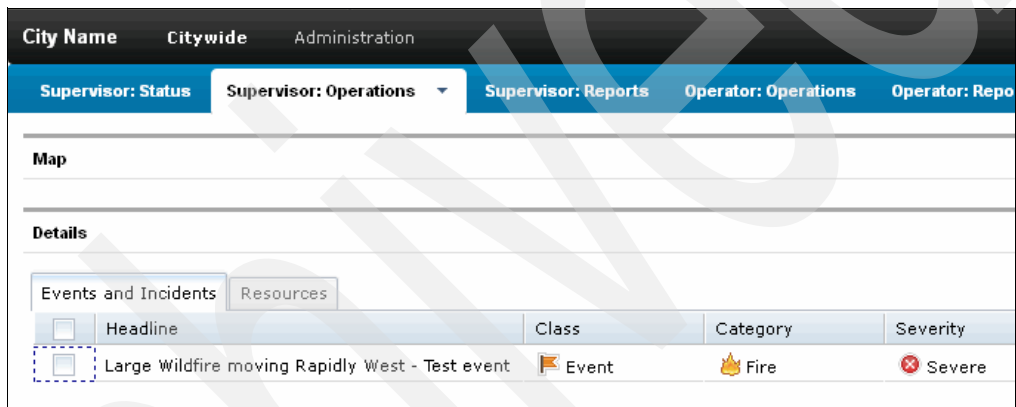


Figure 3-18 Test CAP event in the user interface

4. To remove the test event from the user interface, right-click the message and select **Cancel Event** (Figure 3-19).

For information about removing events from the database, see 4.2.1, “Database table pruning” on page 88.

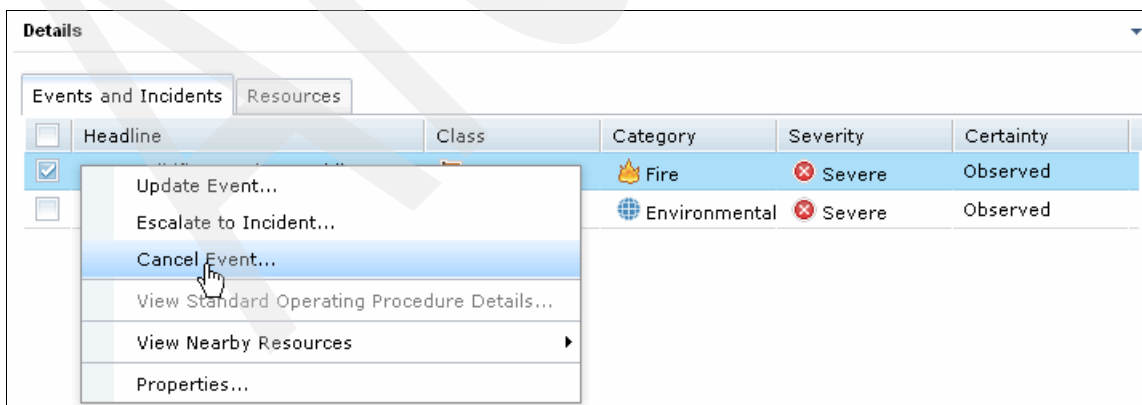


Figure 3-19 Canceling a test event

3.4.2 Creating test KPI messages

This section demonstrates how to use the Sample Event Publisher portlet to generate a test KPI message. Complete the following steps:

1. Start the Sample Event Publisher portlet. In the IBM Intelligent Operations Center, in the left pane, click **Intelligent Operations** → **Demonstration Tools** → **Sample Event Publisher** (see Figure 3-15 on page 60).
2. Click the **Event CAP** tab of the Sample Publisher portlet.
3. To test a KPI message, submit a form like the one shown in Figure 3-20.

The screenshot shows the 'Event CAP' tab of the Sample Event Publisher portlet. The 'Category' dropdown is set to 'All' and the 'Sample Event' dropdown is set to 'Water Quality 1 (KPI: Water Quality)'. The 'Event Message' text area contains the following XML code:

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd
">
  <cap:identifier>Msg25:WaterQualityOne</cap:identifier>
  <cap:sender>Water</cap:sender>
  <cap:sent>2012-07-23T22:00:00-05:00</cap:sent>
  <cap:status>Actual</cap:status>
  <cap:msgType>Alert</cap:msgType>
  <cap:scope>Public</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
    <cap:category>Env</cap:category>
    <cap:event>Water_Quality</cap:event>
    <cap:urgency>Immediate</cap:urgency>
    <cap:severity>Severe</cap:severity>
    <cap:certainty>Observed</cap:certainty>
    <cap:headline>Water Quality</cap:headline>
    <cap:description>Water Quality</cap:description>
    <cap:onset>2012-07-23T22:47:00-05:00</cap:onset>
    <cap:senderName>Water</cap:senderName>
    <cap:parameter>
      <cap:valueName>PH</cap:valueName>
      <cap:value>Take action</cap:value>
    </cap:parameter>
    <cap:parameter>
      <cap:valueName>Turbidity</cap:valueName>
      <cap:value>acceptable</cap:value>
    </cap:parameter>
  </cap:info>
</cap:alert>
```

Figure 3-20 Generating a test KPI message

Select or update the values as follows:

Category	All.
Sample Event	Water Quality 1 (KPI:Water Quality).
<cap:sent>	Update this element to a value within two hours of the time when the message is sent.
<cap:code:>	This value is KPI, which indicates that this message is a KPI. Do not change this value.

- <cap:onset>** For this sample event, update this element to a value within two hours before the time when the message is sent.
- <cap:value>** Take action. The KPI is displayed in the color red.

<cap:value> element: The <cap:value> element for <cap:valueName>PH</cap:valueName> sets the KPI colors as follows:

- ▶ Acceptable = green
- ▶ Caution = yellow
- ▶ Take action = red

4. Select **Randomized Events**, as shown in Figure 3-17 on page 61, to ensure that the identifier is unique. Click **Submit Event**.
5. Verify that the event is displayed in the IBM Intelligent Operations Center GUI:
 - a. Click **Citywide** → **Supervisor: Status**.
 - b. The test KPI message in this example is *Water Quality* and the PH value is *Take Action*, so the color is red (Figure 3-21).

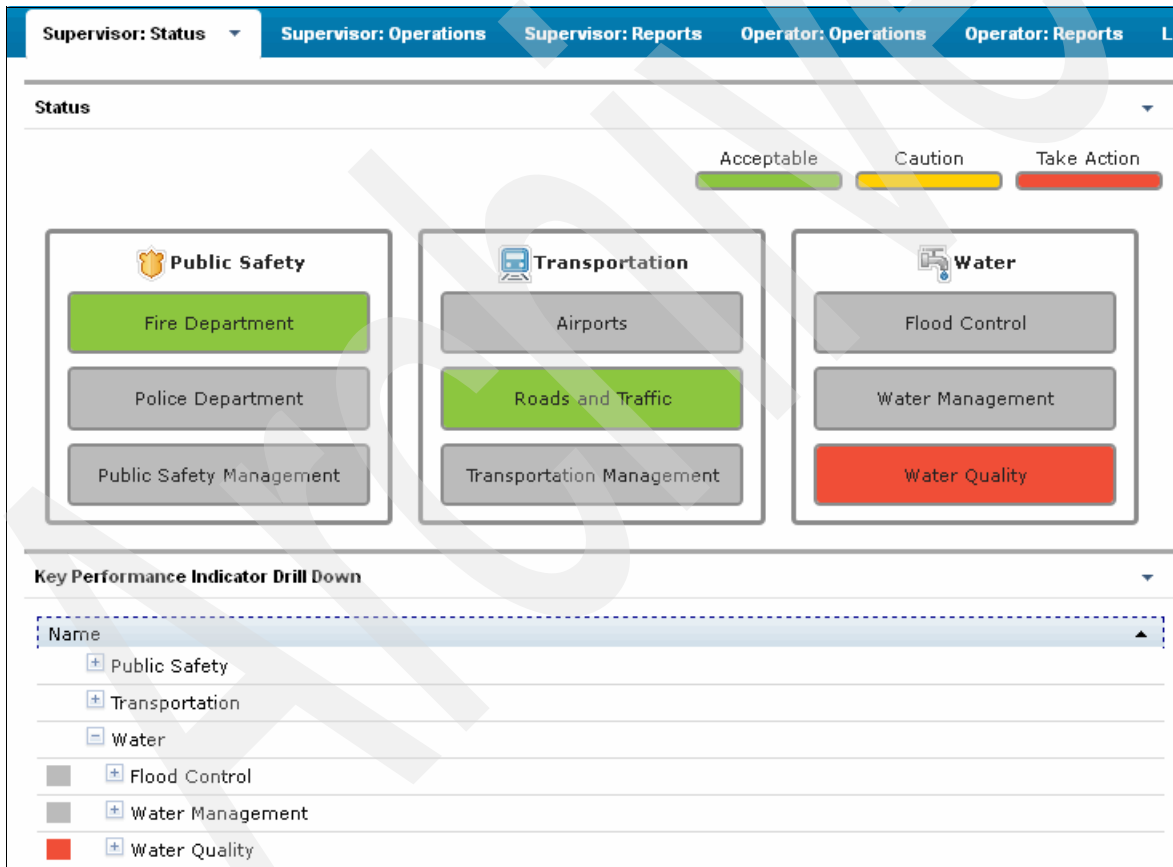


Figure 3-21 Test KPI message that is displayed in the user interface

6. Drill down to display the KPI drill-down (Figure 3-22).

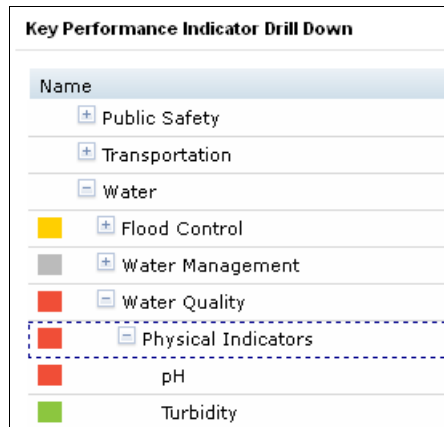


Figure 3-22 KPI drill-down

For information about removing the KPIs and pruning the database, see 4.2.1, “Database table pruning” on page 88.

3.4.3 Creating test notifications

This section demonstrates how to use the Sample Event Publisher portlet to generate a test notification message. Complete the following steps:

1. Start the Sample Event Publisher portlet. In the IBM Intelligent Operations Center, in the left pane, click **Intelligent Operations** → **Demonstration Tools** → **Sample Event Publisher** (see Figure 3-15 on page 60).
2. Click the **Notification** tab.
3. To activate a flow of a sample notification message into the system, submit a form like the one shown in Figure 3-23. Click **Submit Notification**.

Sample Event Publisher	
Event CAP Event Form Notification	
Complete this form to submit a notification for specified groups.	
Type	Alert
Category	Fire - Fire suppression and rescue
Headline	Test notification
Description	Notification message tests the notification flow
Sender	Sample Publisher
Sent To Groups	;CityWideOperator;CityWideExecutive;
Refers to Alerts	
Refers to KPIs	
<input type="button" value="Submit Notification"/>	

Figure 3-23 Generating a test notification message

Tip: The values that you enter in the Sent To Groups field must match existing user groups, for example, CityWideOperator and CityWideExecutive, because only matching alerts are displayed in the Coordinator - Alerts portlet list.

4. Verify that the notification is displayed in the IBM Intelligent Operations Center GUI by clicking **Citywide** → **Operator: Operations**. The test notification message in this example is displayed (Figure 3-24).

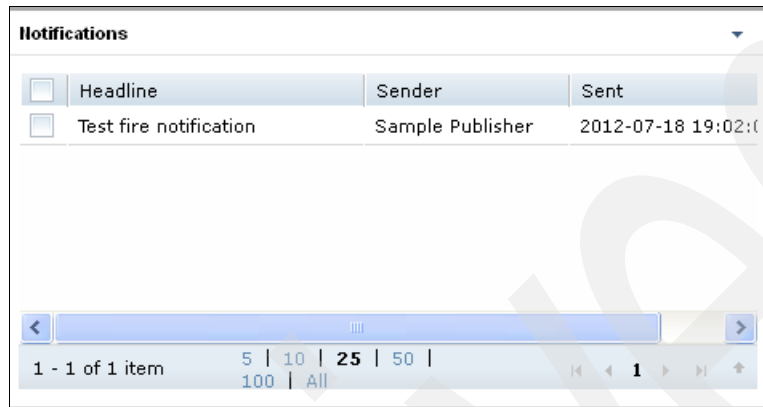


Figure 3-24 Test notification message in the user interface

5. To remove the test notification from the user interface, right-click the message and select **Close Alert** (Figure 3-25).

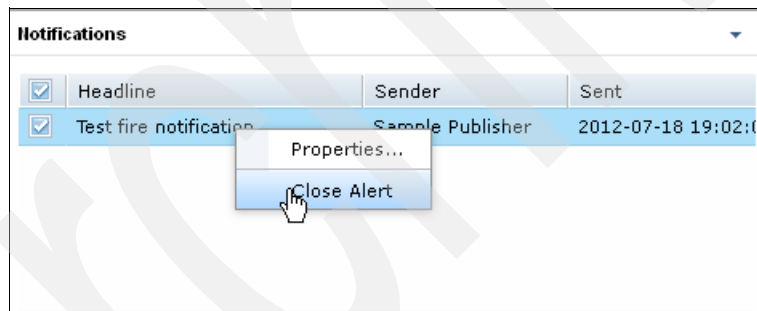


Figure 3-25 Closing an alert and removing the notification from the user interface

For information about removing the notifications from the database, see 4.2.1, “Database table pruning” on page 88.

3.5 System monitoring

IBM Intelligent Operations Center includes a system monitoring service. IBM Tivoli Monitoring monitors key resources and applications on the system. There are several agents that monitor resources on the IBM Intelligent Operations Center servers, including:

- ▶ Linux OS
- ▶ HTTP servers
- ▶ Application servers
- ▶ Disk space

- ▶ Processor utilization
- ▶ Memory

You can start the Tivoli Enterprise Portal from the IBM Intelligent Operations Center Administration Consoles by completing the following steps:

1. Log in to IBM Intelligent Operations Center.
2. In the left pane, expand **Intelligent Operations** → **Administration Tools**.
3. Click **Administration Consoles**. The page opens (see Figure 3-13 on page 56).
4. Click **Application Monitoring** (Figure 3-26).

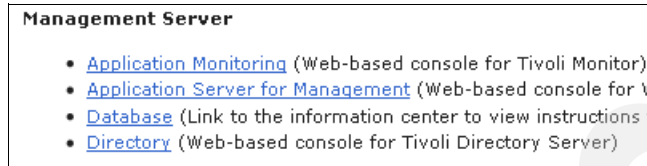


Figure 3-26 Administration Consoles - Application Monitoring

5. On the IBM Tivoli Monitoring Service Index window, click **IBM Tivoli Enterprise Portal Web Client** (Figure 3-27).



Figure 3-27 IBM Tivoli Monitoring Service Index

6. The Tivoli Enterprise Portal starts (Figure 3-28).



Figure 3-28 Tivoli Enterprise Portal logon

Starting the web console: The first time that you start the Tivoli Enterprise Portal web console, a Java plug-in is installed. Make sure that you notice and allow pop-up menus on your web browser.

With its initial settings, you can use the Tivoli Enterprise Portal console to look at processor utilization, memory, disk space, and so on. IBM Tivoli Monitoring can be extended by creating *situations*. For example, to send email alerts whenever there is a disk space issue or the processor utilization is above a certain threshold. For information about IBM Tivoli Monitoring customization, see the product documentation at the following website:

http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.1/welcome.htm

The first time you start the Tivoli Enterprise Portal after the IBM Intelligent Operations Center installation, you notice several red alerts triggered by situations that you can ignore. Figure 3-29 shows an example of a false alert.

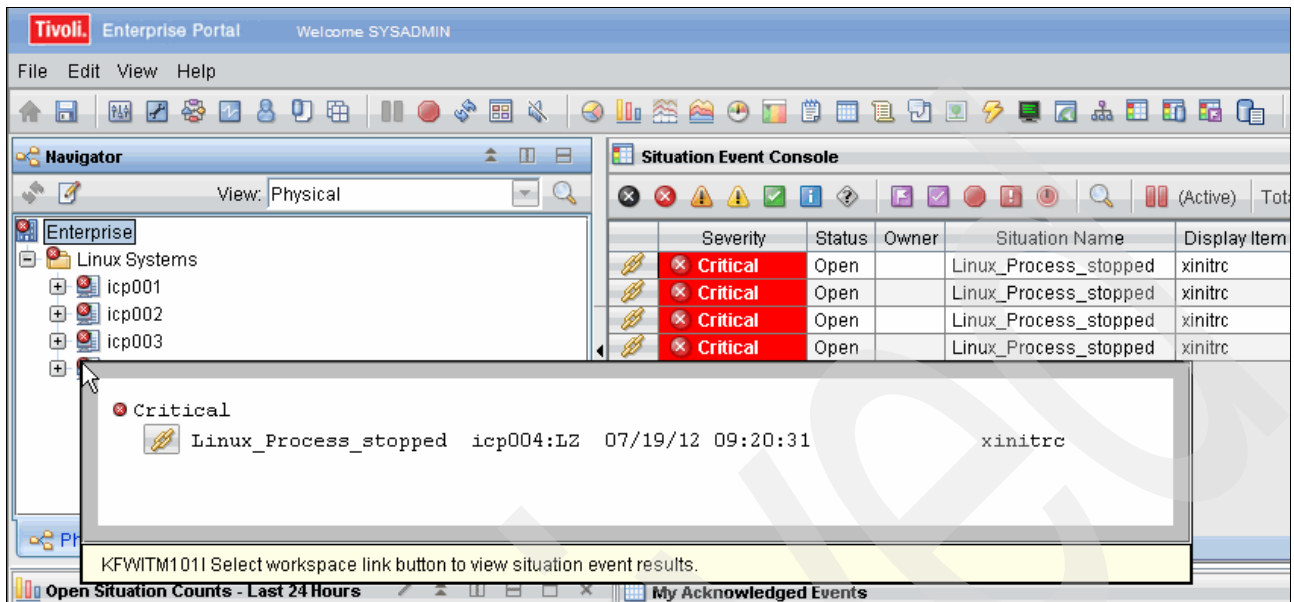


Figure 3-29 False alert that is caused by a process that stops

To reset the alerts after the IBM Intelligent Operations Center installation, right-click the alert and select **Stop Situation** (Figure 3-30).

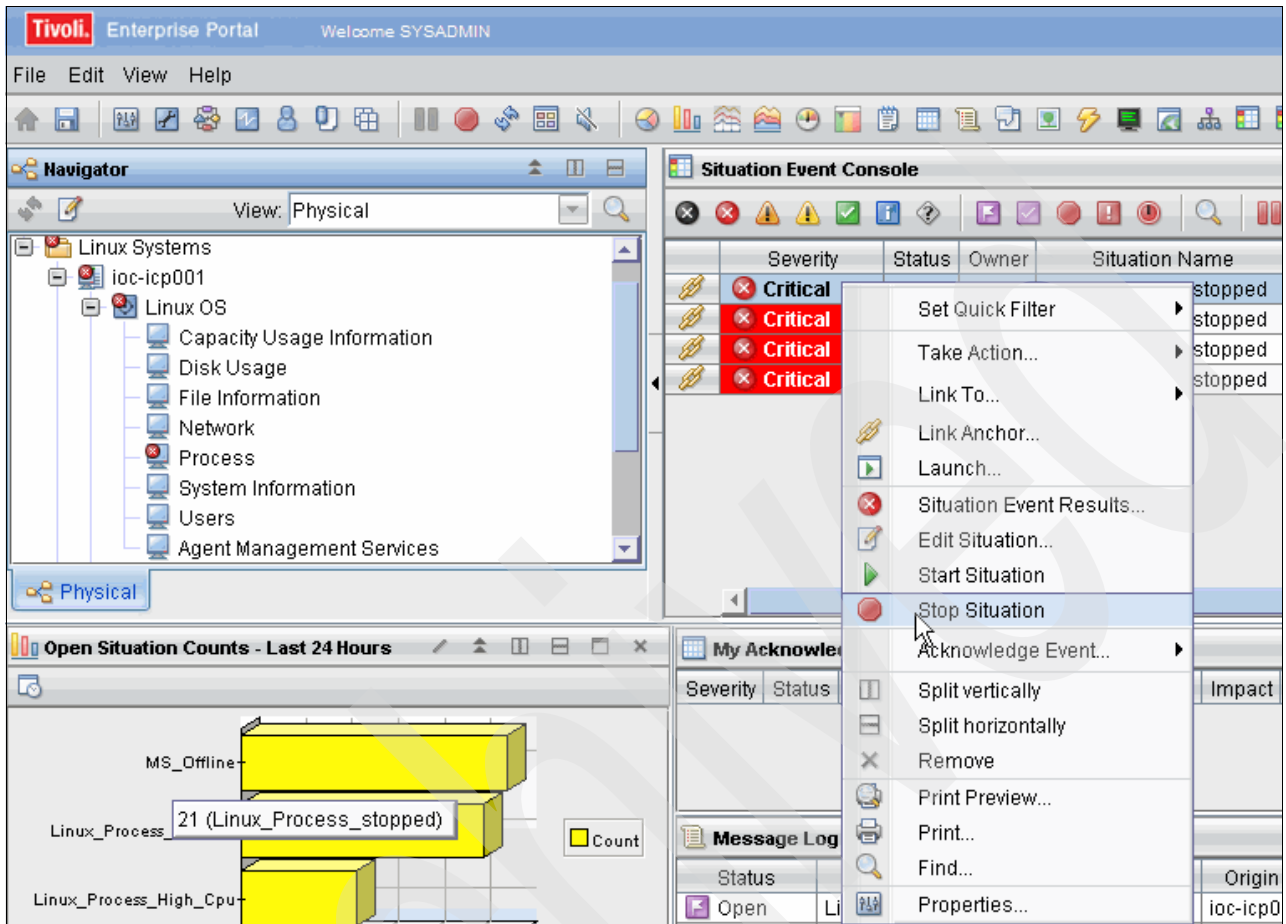


Figure 3-30 Resetting critical alerts after the initial installation

For each IBM Intelligent Operations Center server, you can see all the agents that are installed. Clicking **Linux OS** shows the current processor usage, disk I/O transfers, and system load for that server (Figure 3-31).

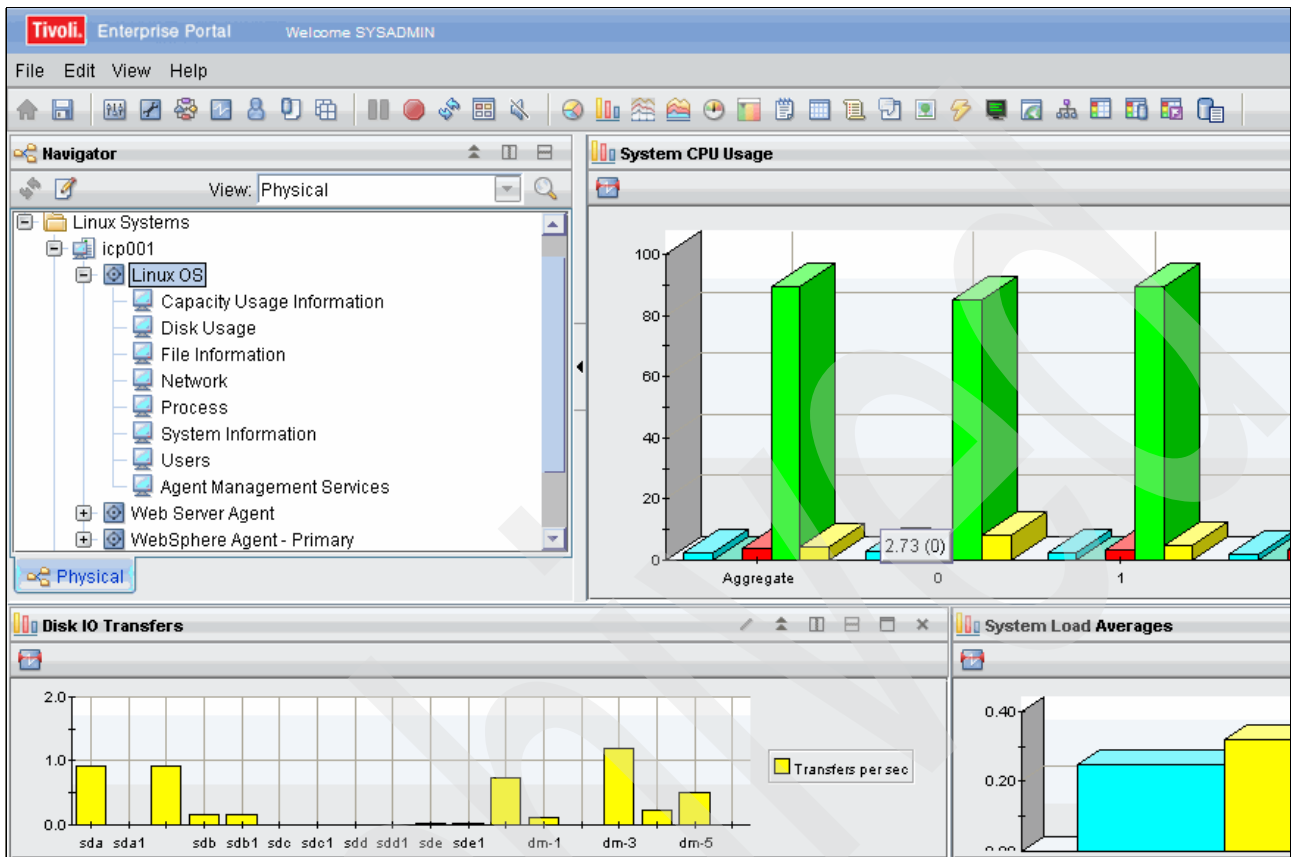


Figure 3-31 System usage, disk I/O, and average system load

You can display the logs for the applications that are monitored by clicking **Log Analysis** (Figure 3-32).

The screenshot shows the Tivoli Enterprise Portal interface. The top bar includes the Tivoli logo and 'Enterprise Portal' text. Below the menu bar, there is a Navigator pane on the left showing a tree view of system components. The 'Log Analysis' option is selected and highlighted. The main content area displays a table of log events. The table has the following columns: Error Date and Time, Thread ID, Severity, Message ID, Message Text, and ASII. The data rows show informational messages from the Transport Channel Service, including details about TCP channels listening on various ports and the start of different service chains.

Error Date and Time	Thread ID	Severity	Message ID	Message Text	ASII
07/18/12 18:51:33	0000...	Informational	CHFW0019I	The Transport Channel Service has started chain WCInboundAdmin.	N/A
07/18/12 18:51:33	0000...	Informational	TCPC0001I	TCP Channel TCP_2 is listening on host * (IPv4) port 9081.	N/A
07/18/12 18:51:33	0000...	Informational	CHFW0019I	The Transport Channel Service has started chain WCInboundDefault.	N/A
07/18/12 18:51:33	0000...	Informational	CHFW0019I	The Transport Channel Service has started chain HttpQueueInboundDefault.	N/A
07/18/12 18:51:33	0000...	Informational	TCPC0001I	TCP Channel TCP_4 is listening on host * (IPv4) port 9444.	N/A
07/18/12 18:51:33	0000...	Informational	CHFW0019I	The Transport Channel Service has started chain HttpQueueInboundDefault...	N/A
07/18/12 18:51:33	0000...	Informational	TCPC0001I	TCP Channel TCP_3 is listening on host * (IPv4) port 9045.	N/A
07/18/12 18:51:33	0000...	Informational	CHFW0019I	The Transport Channel Service has started chain WCInboundAdminSecure.	N/A

Figure 3-32 Log analysis for IBM Tivoli Directory Server

Figure 3-33 shows the status of the applications that are running in the portal server.

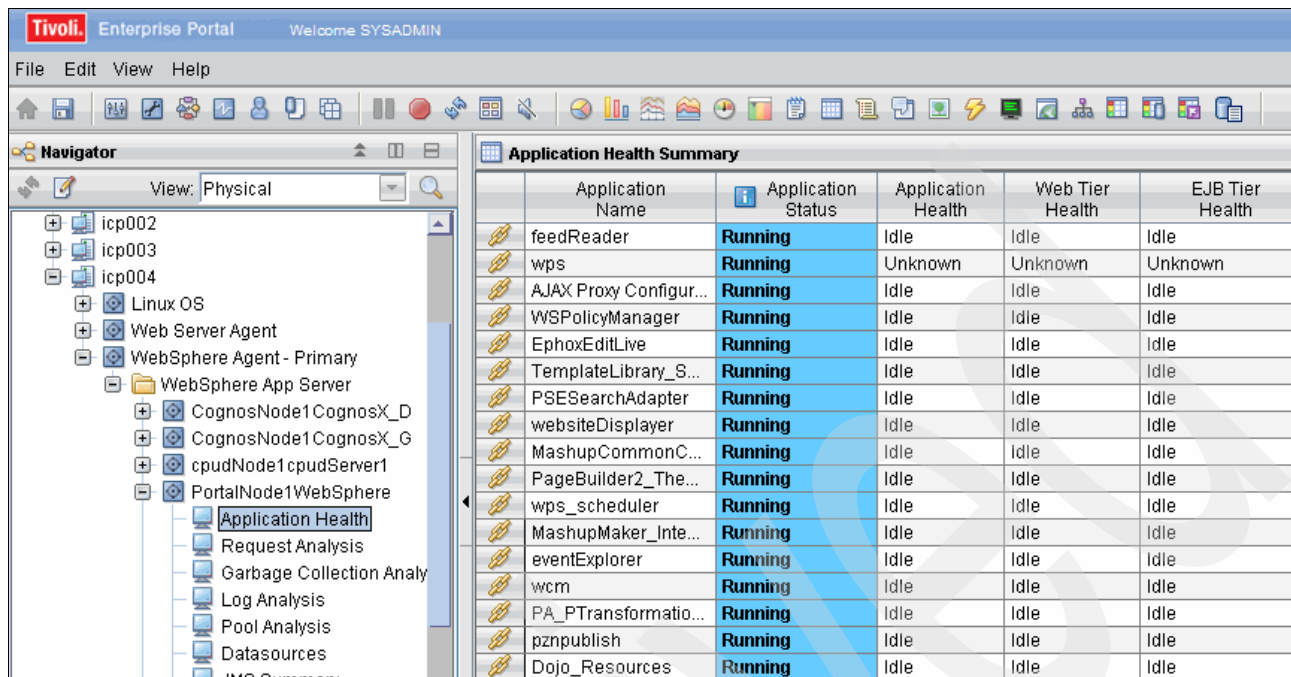


Figure 3-33 Portal server application health

For more information, see the *Tivoli Enterprise Portal User's Guide*, found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itm.doc_6.2.2fp2/itm622fp2_tepuser.htm

3.6 WebSphere MQ Explorer

WebSphere MQ Explorer is a graphical tool that you can use to check the IN and OUT queues for the services that are described in Chapter 2, “Topology” on page 23 and Chapter 7, “Data flows” on page 189.

To start WebSphere MQ Explorer, run the following commands on the event server using a graphical terminal emulator such as Virtual Network Computing (VNC):

```
xhost +
su - mqm
/usr/bin/strmqcfg
```

Exiting WebSphere MQ Explorer: After exiting WebSphere MQ Explorer, to switch back to the root user, run `exit`. To turn access control on again, run `xhost -`.

WebSphere MQ Explorer starts and the welcome page is displayed (Figure 3-34).



Figure 3-34 Starting WebSphere MQ Explorer

Close the Welcome page and click **Queue Managers** to display the IBM Intelligent Operations Center queue manager status (Figure 3-35).

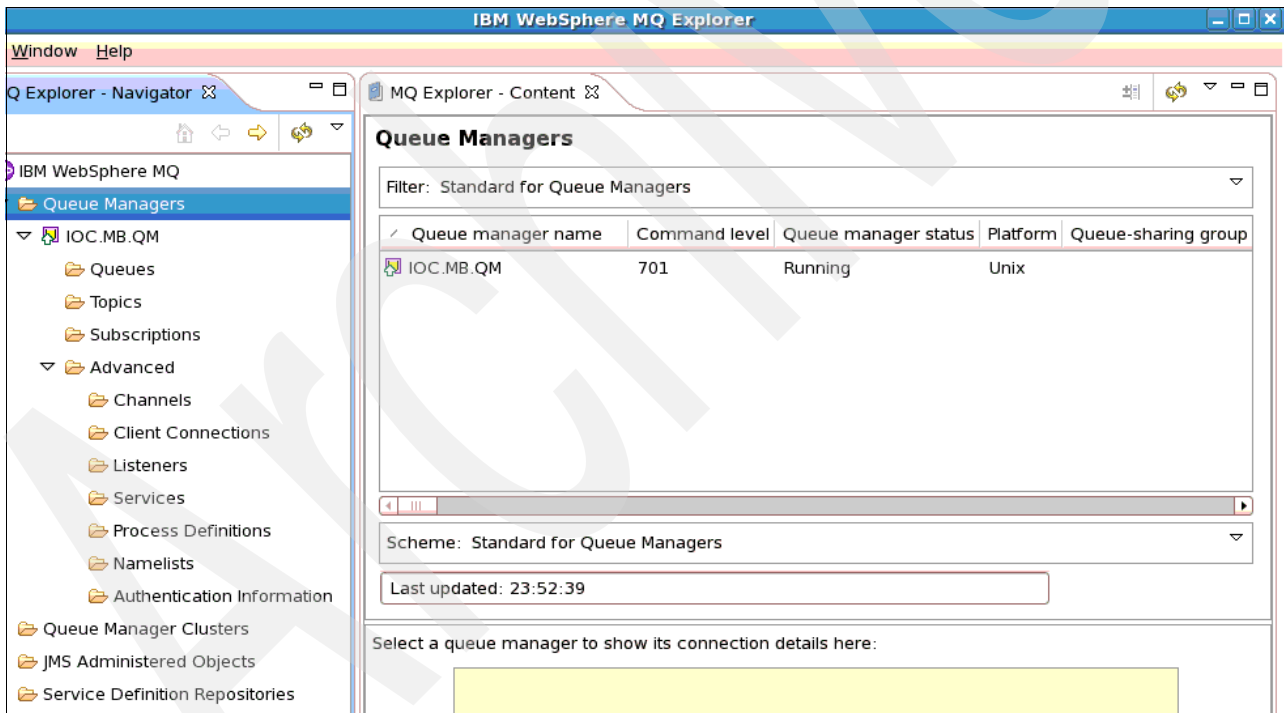


Figure 3-35 IBM Intelligent Operations Center queue manager status

To check the total number of messages in a queue, from the left pane, click **Queues**. Look at the number under the Current queue depth column for the queue (Figure 3-36).

The screenshot shows the 'Queues' section of the MQ Explorer interface. A filter is set to 'Standard for Queues'. A table lists various queues with their current and maximum depths. The queue 'IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY' is highlighted in blue.

Queue name	Queue type	Current queue depth	Max queue depth
DEAD.LETTER.Q	Local	0	5000
DEAD.MESSAGE.Q	Local	2	5000
IOC_CAP_OUT_INTERNAL_USE_ONLY_DO_NOT_MOI	Local	0	5000
IOC_JRULES_IN_INTERNAL_USE_ONLY_DO_NOT_MO	Local	0	5000
IOC_JRULES_OUT_INTERNAL_USE_ONLY_DO_NOT_M	Local	9	5000
IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY	Local	0	5000
IOC_KPI_OUT_INTERNAL_USE_ONLY_DO_NOT_MOD	Local	0	5000
IOC_KPI_UPDATE_INTERNAL_USE_ONLY_DO_NOT_M	Local	0	5000
IOC_NOTIFICATION_IN_INTERNAL_ONLY_DO_NOT_M	Local	0	5000
IOC_NOTIFICATION_OUT_INTERNAL_ONLY_DO_NOT	Local	0	5000
IOC_RESOURCE_IN_INTERNAL_USE_ONLY_DO_NOT	Local	0	5000
IOC_RESOURCE_OUT_INTERNAL_USE_ONLY_DO_N	Local	0	5000
IOC.CAP.IN	Local	0	5000
IOP.CAT.REQ	Local	0	5000
IOP.CAT.RSP	Local	0	5000

Below the table, the scheme is 'Standard for Queues - Distributed' and the last update time is '23:58:18'.

Figure 3-36 Checking the number of messages in the queues

For examples of using WebSphere MQ Explorer in troubleshooting scenarios, see Chapter 6, “Troubleshooting” on page 137.

3.7 Database control center

You might want to view the IBM Intelligent Operations Center solution database when you troubleshoot a message flow or information that is displayed on the portal. This section addresses the operation of DB2 database control center for the IOCDDB database that stores all the solution-based information. The other subsystem databases can be treated in the same way using the appropriate database instance name and navigating through its database tables. For the list of the IBM Intelligent Operations Center databases, see Table 4-3 on page 90.

The database control center is on the data server. To start the database control center and navigate to a table, complete the following steps:

1. Log in to the data server as root.
2. Switch the user to the appropriate database instance (see Table 5-1 on page 102 for database instance user IDs). For the IOCDDB database, the instance is db2inst1. Run the following commands:

```
xhost +  
su - db2inst1
```

Exiting the database control center: After you exit the database control center, to switch back to the root user, run `exit`. To turn access control on again, run `xhost -`.

3. To open the DB2 control center, run the following command:

```
db2cc
```

4. In the DB2 control center, click **All Databases** → **IOCDDB** → **Tables**. Figure 3-37 shows the EVENT table that is selected from the tables list in DB2 control center.

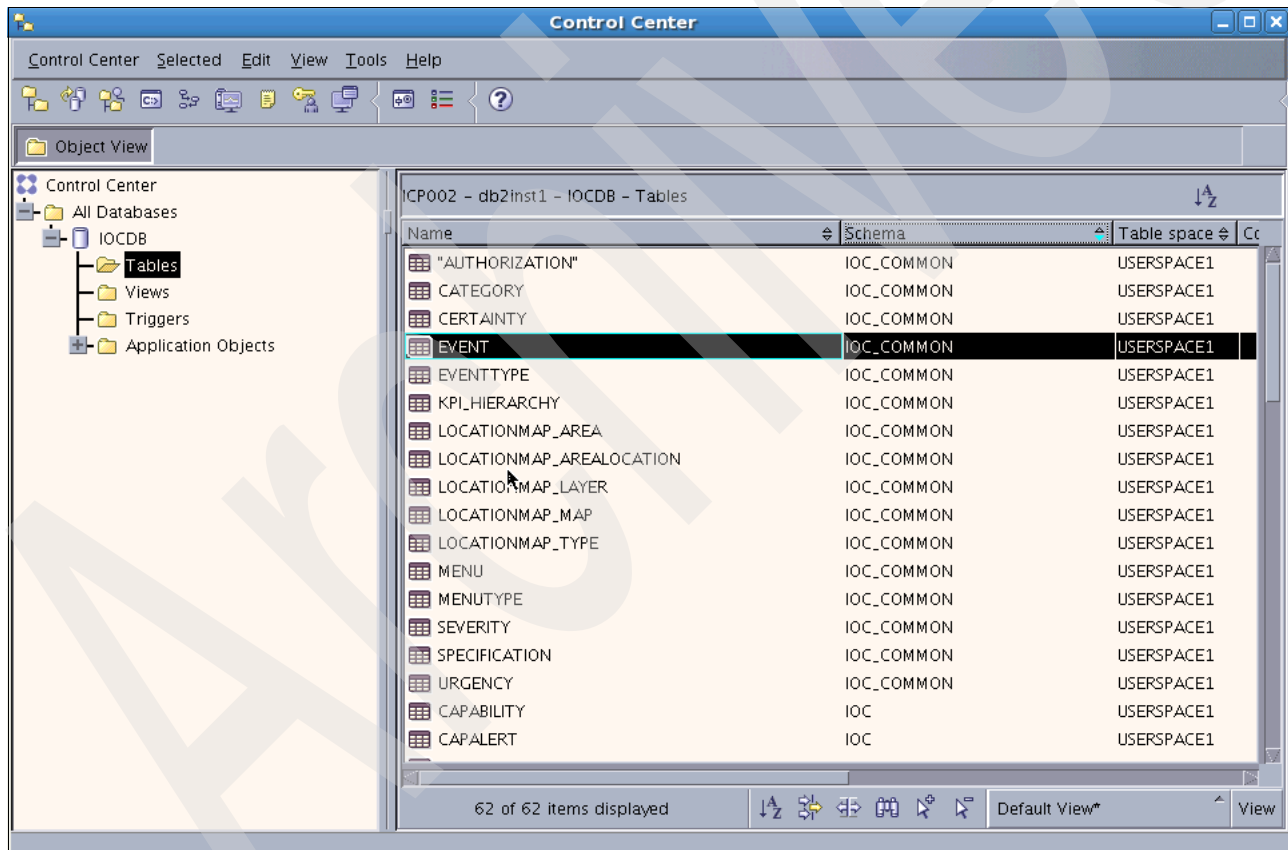


Figure 3-37 Database control center view

5. Double-click the chosen table, the EVENT table in this example, and view the contents of the table.
6. To import or export the contents of a table, right-click the table name and specify the output file location.

For more information about the DB2 Control Center, see the IBM DB2 Universal Database™ Information Center at:

<http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp>

3.8 IBM Tivoli Netcool/OMNIBus database utility

You might need to view the NCOMS ObjectServer databases when troubleshooting message flow problems, as described in Chapter 6, “Troubleshooting” on page 137. You must run the **nco_config** utility to start the Netcool/OMNIBus Administrator. To start the Netcool/OMNIBus Administrator from the command line, complete the following steps on the event server:

1. Run **/opt/IBM/netcool/omnibus/bin/nco_config**. Netcool/OMNIBus Administrator starts (Figure 3-38).

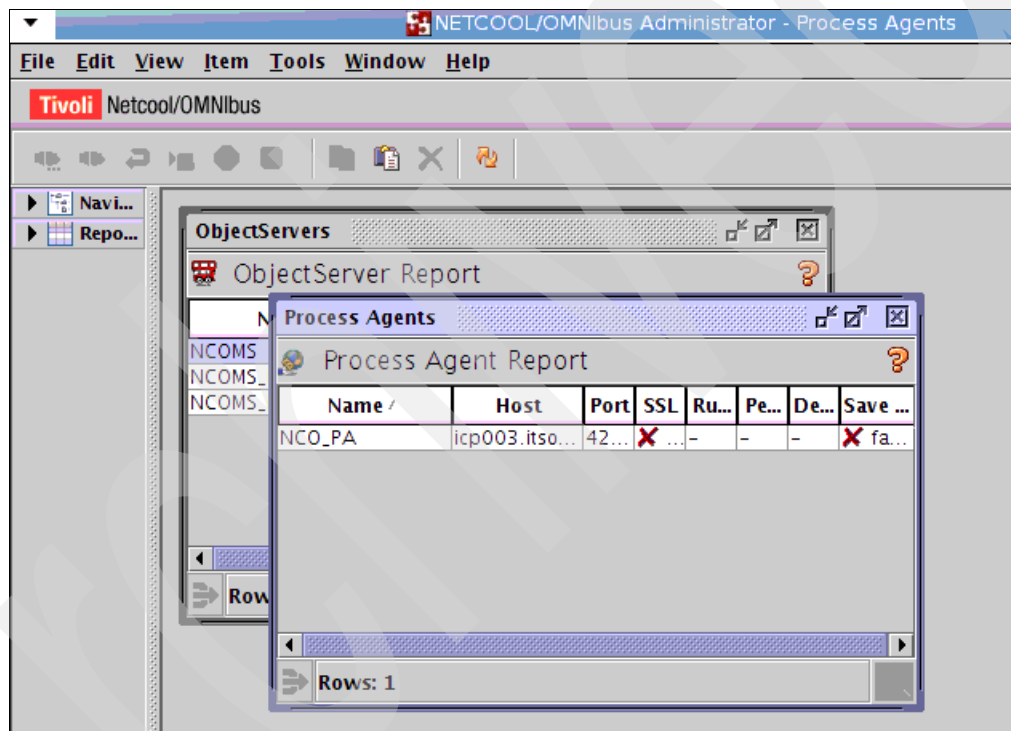


Figure 3-38 Starting Tivoli Netcool/OMNIBus Administrator

Import Connections wizard: The first time you start Netcool/OMNIBus Administrator, the Import Connections wizard runs. Click **Next** on each window without making any changes. On the last window that opens, click **Finish**.

2. On the **ObjectServers** window, right-click **NCOMS** and select **Connect As...** (Figure 3-39).

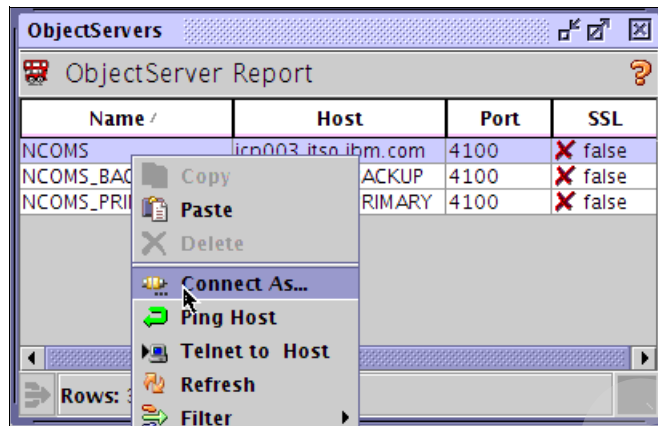


Figure 3-39 Connecting to NCOMS ObjectServer (1 of 2)

Tip: If the ObjectServers window does not open automatically, click **View** → **ObjectServers**.

3. Log in as root and click **OK** (Figure 3-40).

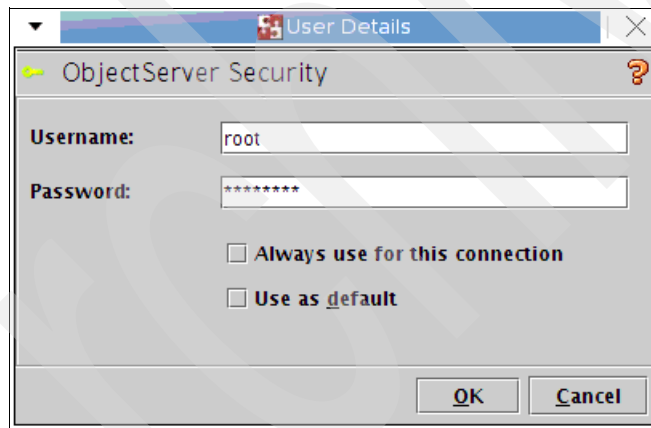


Figure 3-40 Connecting to NCOMS ObjectServer (2 of 2)

- Expand **System**, click **Databases**, and expand **Alerts**. You can browse the tables in the alerts database (Figure 3-41).

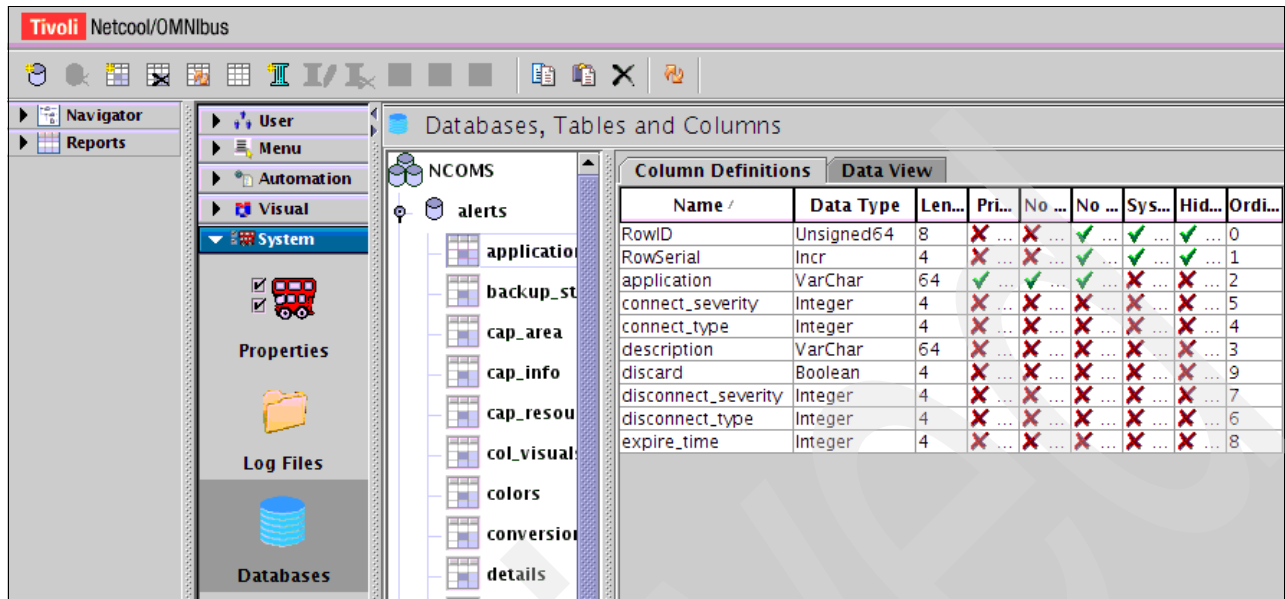


Figure 3-41 Browsing NCOMS databases

For examples about how to use Tivoli Netcool/OMNibus Administrator in problem determination scenarios, see 6.1, “Troubleshooting scenarios” on page 138.

3.9 MustGather tool

IBM Intelligent Operations Center provides a *MustGather* tool that you can use to gather log files and other information that is required to analyze problems with the installation or usage of the solution.

Netcool administration: The Netcool administration portal can be viewed by using the administration consoles described in 3.3, “Administration Consoles” on page 55 and selecting **Event Handling**. The MustGather tool described in this section does not address the Netcool administration portal.

To run the MustGather Tool from the installation server, complete the following steps:

- Open a terminal window and log in as root or administrator.
- Change to the <install-home>/ioc/bin directory. In our test environment, the <install-home> directory is /opt/IBM/IOC/BA. Run the following command:

```
cd /opt/IBM/IOC/BA/ioc/bin
```
- Set the JAVA_HOME variable to point to your Java 6 runtime JRE. Run the following command:

```
export JAVA_HOME=/opt/ibm/java-x86_64-60/jre
```
- Run the **mustgather** script, where <password> is your administration password:

```
./mustgather.sh -p <password>
```

Example 3-1 shows the output of running the `mustgather.sh` script.

Example 3-1 Running the mustgather.sh script

```
[root@icp000 bin]# ./mustgather.sh -p ibmdop20
CIYBA0233I: Current topology is "iop_lite_topo_mustGather".
[17:31:15] CIYBA0254I: Install component [APP_HOST_1] on host
[icp004.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:22] CIYBA0254I: Install component [EVENT_HOST_1] on host
[icp003.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:22] CIYBA0254I: Install component [MGMT_HOST_1] on host
[icp001.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:22] CIYBA0254I: Install component [DB_HOST_1] on host
[icp002.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:25] CIYBA0254I: Install component [mustGather_e1] on host
[icp003.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:38] CIYBA0254I: Install component [mustGather_d1] on host
[icp002.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:38] CIYBA0254I: Install component [mustGather_m1] on host
[icp001.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:38] CIYBA0254I: Install component [mustGather_a1] on host
[icp004.itso.ibm.com] [ CIYBA0259I: OK ]
[17:31:53] CIYBA0240I: Command finished successfully.
```

Tip: The first time you run the MustGather tool, it scans your installation properties file. If you modify the installation properties file after running the MustGather tool, use the `-n` option the next time you run the tool. The tool rescans your modified properties file. The command with the `-n` option is:

```
./mustgather.sh -n -p <password>
```

5. Locate the resulting files in the following directory on the installation server.

```
/installMedia/mustGather
```

There is one `.tar` file for each of the target servers and one for the installation server that contains the log files and other information needed to analyze the issues.

Example 3-2 shows the resultant `.tar` files gathered by the MustGather tool.

Example 3-2 Results of MustGather tool

```
CIYBA0239E: If you want more detailed operation messages, please check
/opt/IBM/IOC/BA/ioc/log/installTopology_iop_lite_topo_mustGather_20120726_1731.
log.
mustGather/
mustGather/icp000.itso.ibm.com_26Jul2012_17-31-53.tar
mustGather/icp004.itso.ibm.com_26_07_2012_05_31_PM.tar
mustGather/icp003.itso.ibm.com_26_07_2012_05_31_PM.tar
mustGather/icp001.itso.ibm.com_26_07_2012_05_31_PM.tar
mustGather/icp002.itso.ibm.com_26_07_2012_05_31_PM.tar
please submit the following file
/tmp/iop-install-mustgather.26Jul2012_17-31-53.tar
```

3.10 System-wide configuration properties

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data. For information about the system-wide properties table, see the “Specifying system-wide configuration data” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/extend_sysprop.html

To change system-wide IBM Intelligent Operations Center configuration data, update the system properties table. For information about the procedure to update the systems properties table, see the “Updating the system properties table” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/extend_edit_sysprop.html

3.11 Solution logs

Some troubleshooting procedures direct you to look at log files. For information about the log file locations for each IBM Intelligent Operations Center server, see the “Troubleshooting the components” topic in IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/ts_components.html

All the log files are created automatically. You can view them by running the appropriate `tail` commands.

Table 3-3 lists the log files for the IBM Intelligent Operations Center components that run on the application server.

Table 3-3 Application server components and log files

Component	Log files
IBM Cognos Administration	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemErr.log ▶ /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log ▶ All logs in the /opt/IBM/cognos/c10_64/logs/ directory
IBM HTTP Server	<ul style="list-style-type: none"> ▶ /opt/IBM/HTTPServer/logs/error_log ▶ /opt/IBM/HTTPServer/logs/access_log
IBM WebSphere Business Monitor	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
IBM Lotus Sametime Proxy Server	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
Tivoli Access Manager	<ul style="list-style-type: none"> ▶ /var/pdweb/log/msg_*.log, where * is any value ▶ /var/pdweb/log/config_data_*.log, where * is any value

Component	Log files
Tivoli Access Manager WebSEAL	<ul style="list-style-type: none"> ▶ /var/pdweb/log/msg__webseald-default.log ▶ All logs in the /var/pdweb/www-default/log/ directory
Tivoli Directory Server Proxy configuration log	/datahome/proxy/idsslapd-tdsproxy/logs/ibmslapd.log
WebSphere Operational Decision Manager	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
WebSphere Portal	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log ▶ /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
WebSphere UDDI Registry	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log

Table 3-4 lists the log files for the IBM Intelligent Operations Center components that run on the data server.

Table 3-4 Data server components and log files

Component	Log files
DB2	/datahome/<instance name>/sql/lib/log
Tivoli Directory Server	<ul style="list-style-type: none"> ▶ /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log ▶ All logs in the /datahome/dsrdbm01 /idsslapd- dsrdbm01/logs/ directory

Table 3-5 lists the log files for the IBM Intelligent Operations Center components that run on the event server.

Table 3-5 Event server components and log files

Component	Log files
Lotus Domino	<ul style="list-style-type: none"> ▶ /local/notesdata/console.out ▶ /local/notesdata/log.nsf ▶ All logs in the /local/notesdata/IBM_TECHNICAL_SUPPORT/ directory.
Lotus Sametime Community Server	To collect and write all pertinent log files to the /local/notesdata/ directory, run the following command: /local/notesdata/sh stdiagzip.sh
Tivoli Netcool/Impact	<ul style="list-style-type: none"> ▶ /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log ▶ /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
Tivoli Netcool/OMNibus	<ul style="list-style-type: none"> ▶ /opt/IBM/netcool/log ▶ /opt/IBM/netcool/omnibus/log
Tivoli Service Request Manager	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log
WebSphere MQ	<ul style="list-style-type: none"> ▶ /var/mqm/errors/AMQERR*.LOG ▶ /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Table 3-6 lists the log files for the IBM Intelligent Operations Center components that run on the management server.

Table 3-6 Management server components and log files

Component	Log files
Management server	<ul style="list-style-type: none"> ▶ Tivoli Event Monitoring Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log ▶ Tivoli Event Portal Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log ▶ Embedded WebSphere Application Server logs: <ul style="list-style-type: none"> – Error log: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log – Output log: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log – Start log: /opt/IBM/ITM/1i6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log
Tivoli Access Manager and WebSphere Portal Manager	<ul style="list-style-type: none"> ▶ /var/PolicyDirector/log/msg__pdmgrd_utf8.log ▶ /var/PolicyDirector/log/msg__pdacld_utf8.log
Tivoli Access Manager	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
Tivoli Enterprise Monitoring Agent	/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log
Tivoli Enterprise Portal	/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log
Tivoli Identity Manager	<ul style="list-style-type: none"> ▶ /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log ▶ /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log ▶ All logs in V6 subdirectories of the /var/idsldap/ directory

3.12 Checking the health of the solution

It is a preferred practice to verify the health of the system daily as follows:

1. Run the System Verification Check All tests, as described in 3.2, “System Verification Check” on page 48.
2. Navigate the IBM Intelligent Operations Center portal interface to make sure all the business portlets display correctly.

Preventive maintenance

This chapter provides information about basic administrative tasks that IBM Intelligent Operations Center administrators must perform at regular intervals to keep the solution infrastructure healthy.

Topics that are covered in this chapter include:

- ▶ 4.1, “Backing up and archiving log files” on page 84 includes information about automating log archiving to keep historical records and control the log files’ size.
- ▶ 4.2, “Database maintenance” on page 86 includes information about monitoring and pruning of database tables.
- ▶ 4.3, “Backing up and restoring” on page 90 explains a simple approach to back up and restore the entire IBM Intelligent Operations Center solution environment.
- ▶ 4.5, “Tivoli Enterprise Portal” on page 97 describes a monitoring tool that provides information about the system. This tool is useful for both monitoring the health of the overall system and troubleshooting issues that the system might be experiencing.

4.1 Backing up and archiving log files

Maintenance of log files is an important task to keep your system operating properly. Correct maintenance of these files offers many advantages, including performance improvements. For example, when you try to determine the cause of a problem or determine the existing configuration of a particular component, a clean log file system helps with reading through all the existing entries. This section covers both the backup and restore of log files.

4.1.1 Backing up log files

The backup process is used to store multiple versions of log files on a separate backup system. If there is an issue where you lose your data, a backup of any problem information is available to you on the backup server.

The following steps describe how to perform the backup of the portal log files. Similar steps can be performed to back up other log files. You can find more information about the location of IBM Intelligent Operations Center log files in 3.11, “Solution logs” on page 80.

1. Log in to the application server as root.
2. Go to the location where the portal log files are stored:

```
$ cd /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal
```
3. From the command line, run the **tar** command to bundle the files and create the compressed file:

```
$ tar -cjf portal-logs-`date +%Y-%m-%d`.tar.bz2 *.log
```
4. Run **rsync** to copy the archived logs to the backup server:

```
$ rsync portal-logs-`date +%Y-%m-%d`.tar.bz2 user@<Backup Server>:/backup-folder/
```

Important: <Backup Server> is not part of IBM Intelligent Operations Center.

5. Clean up the transferred file by running the following command:

```
$ rm portal-logs-`date +%Y-%m-%d`.tar.bz2
```

After you have the necessary commands to back up all instances, you can automate the process by completing the following steps. Example 4-1 illustrates a sample script that automates the process.

Example 4-1 Sample script to automate the backup of the log files

```
#!/bin/bash
FILE=portal-logs-`date +%Y-%m-%d-%H%M%S`.tar.bz2
cd /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal
tar -cjf $FILE *.log
rsync FILE <user>@<Backup Server>:/backup-folder/
rm $FILE
```

1. On the application server, create a script file in the `/opt/IBM/scripts/` directory by running the following commands:

```
$ cd /opt/IBM/  
$ mkdir scripts  
$ cd scripts  
$ vi log_backup.sh
```

2. Copy and paste the contents from Example 4-1 on page 84 to `log_backup.sh`, save the file, and run the following script:

```
$ sh -x log_backup.sh
```

The output displays as follows:

```
++ date +%Y-%m-%d-%H%M%S  
+ FILE=portal-logs-2012-07-13-094805.tar.bz2  
+ BACKUPSERVER=install  
+ BACKUPUSER=root  
+ cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal  
+ tar -cjf portal-logs-2012-07-13-094805.tar.bz2 native_stderr.log  
native_stdout.log startServer.log stopServer.log SystemErr.log SystemOut.log  
+ rsync portal-logs-2012-07-13-094805.tar.bz2 root@install:/root/backup-folder/  
+ rm portal-logs-2012-07-13-094805.tar.bz2
```

Password storage: For security reasons, do not store passwords on the script source code. The `rsync` command prompts for a password when it connects to the backup system.

To run the script without prompting for password, set up a public key exchange by completing the following steps:

1. On the application server, create the public and private keys (if they do not exist) by running the following commands. `id_rsa` is the private key and `id_rsa.pub` is the public key:

```
$ cd ~/.ssh  
$ ssh-keygen -t rsa
```

Private and public keys: The command prompts for a passphrase, press the Enter key to generate your private and public keys. Do *not* share the private key with anyone! By default your key is saved in `/root/.ssh/id_rsa.pub`.

2. Copy the `id_rsa.pub` to the backup server from the application server. To install the public key on the backup server, log in to the backup server and run the following command:

```
$ cat id_rsa.pub >> ~/.ssh/authorized_keys
```

3. Return to the application server and run the `log_backup.sh` script again. It does not prompt you for a password.

```
$ sh -x log_backup.sh
```

Now you can run the script as often as required. You can use a job scheduler, such as **crontab**, to run the script at specific intervals, as described in the following steps:

1. On the application server, run **crontab** in edit mode to include the script to run daily:

```
$ crontab -e
```

2. Paste the following command at the end of the file:

```
daily sh -x /opt/IBM/scripts/log_backup.sh
```

3. Save and exit.

From now on, your portal logs are backed up daily. The logs are stored on the specified backup server. You can do the same setup for all logs that are generated for all software services of the IBM Intelligent Operations Center.

4.1.2 Archiving log files

The archive process is used to improve system performance by minimizing the log files to an optimal size. There are various log management applications available that can be used. One such utility available on Linux is an application called *Logrotate*. The Logrotate program is a log file manager that rotates the logs based on certain criteria (size or frequency). Example 4-2 illustrates a Logrotate's configuration file.

Example 4-2 Sample Logrotate configuration file

```
/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/*.log {  
    missingok  
    compress  
    notifempty  
    daily  
    rotate 5  
    create 0600 root root  
}
```

To archive the portal logs with Logrotate, complete the following steps:

1. Create a Logrotate configuration file and define the permissions (owner and group) by running the following commands:

```
$ touch /etc/logrotate.d/portal  
$ chmod 644 /etc/logrotate.d/portal  
$ chown root.root /etc/logrotate.d/portal
```
2. Open the configuration file in edit mode by running the following command and copy and paste the sample configuration that is shown in Example 4-2:

```
$ vi /etc/logrotate.d/portal
```
3. Save and exit.

Logrotate now rotates all logs files from the portal log location daily.

4.2 Database maintenance

To ensure optimal operation of the IBM Intelligent Operations Center, monitor the status of the servers, particularly the database server, daily. This section describes how to monitor and maintain the database server and the database instances of the IBM Intelligent Operations Center.

Using the **IOCControl** command, as described in 3.1, “Platform control tool (IOCControl or PCT)” on page 44, determine the status of each of the database servers. To run a status check on the database instances with **IOCControl**, you need the target names of the databases that are shown in Table 4-1 on page 87.

Example 4-3 illustrates how to run a status check on the portal database server. It verifies whether the server is on or off.

Example 4-3 Using IOCControl.sh to check the status of the portal database

```
IOCControl.sh status db24po password
```

If the server is up and running, a successful result message is displayed (Example 4-4); otherwise, the message indicates that the server is offline.

Example 4-4 Successful results after the portal database server status check

```
Executing query command...completed.
  IBM DB2 Enterprise server for Portal Server[ on ]
```

Another way to determine the status of the database is to use the System Verification Check tool. System Verification Check is available through the administration console of the IBM Intelligent Operations Center. Details regarding the System Verification Check tool can be found in 3.2, “System Verification Check” on page 48.

The buttons on the System Verification Check page run various tests on the IBM Intelligent Operations Center services. These include tests to determine the status of the database instances of the IBM Intelligent Operations Center. The status check verifies whether the service is up and running. Figure 4-1 shows a partial view specific to the database instances of the IBM Intelligent Operations Center’s System Verification Check tool.

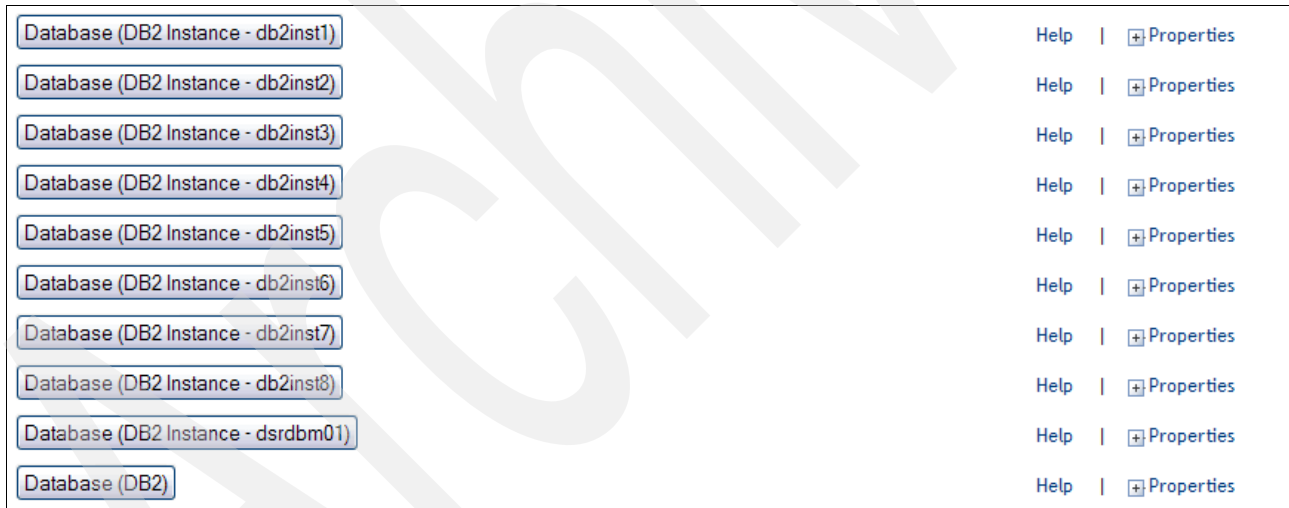


Figure 4-1 System Verification Check - list of database instance tests

See Table 4-1 for information about each System Verification Check test and corresponding IOCControl target when available.

Table 4-1 Database System Verification Check tests and IOCControl targets

System Verification Check test	IOCControl target	Description
Database (DB2 Instance - db2inst1)	db24sol	IBM DB2 Enterprise Server for Solution
Database (DB2 Instance - db2inst2)	db24po	IBM DB2 Enterprise Server for Portal Server
Database (DB2 Instance - db2inst3)	db24ana	IBM DB2 Enterprise Server for Analytics Server

System Verification Check test	IOCControl target	Description
Database (DB2 Instance - db2inst4)	db24wbm	IBM DB2 Enterprise Server for WebSphere Business Monitor
Database (DB2 Instance - db2inst5)	db24sms	IBM DB2 Enterprise Server for Semantic Model Services
Database (DB2 Instance - db2inst6)	db24tsrm	IBM DB2 Enterprise Server for Tivoli Service Request Manager Server
Database (DB2 Instance - db2inst7)	db24mgmt	IBM DB2 Enterprise Server for Management Server
Database (DB2 Instance - db2inst8)	N/A	Application
Database (DB2 Instance - dsrdbm01)	N/A	Directory
Database (DB2)	N/A	Data server

The commands and parameters that are used for the test can be seen by expanding the Properties link on the right of each instance row. If the database instance is active, you see a green icon (Figure 4-2). If the database server is not active, then you see a red icon instead. Details about the tests and test results can be found in the Help link for each test. You can also click either the green or red icon to see the details view of the results.

Database (DB2 Instance - db2inst1)	✓	Help
Database (DB2 Instance - db2inst2)	✓	Help
Database (DB2 Instance - db2inst3)	✓	Help
Database (DB2 Instance - db2inst4)	✓	Help
Database (DB2 Instance - db2inst5)	✓	Help
Database (DB2 Instance - db2inst6)	✓	Help
Database (DB2 Instance - db2inst7)	✓	Help
Database (DB2 Instance - db2inst8)	✓	Help
Database (DB2 Instance - dsrdbm01)	✓	Help
Database (DB2)	✓	Help

Figure 4-2 System Verification Check tool results of the database status check

4.2.1 Database table pruning

There are various database tables that grow as the solution data flows through the system. Some tables are transient, such as the notifications where the user generally cleans up the data table after confirming the notification. Set up a procedure to check if these transient tables are getting too large. If these tables get too large, it affects the performance and operation of the IBM Intelligent Operations Center. It is because of this adverse effect that you perform regular pruning of certain database tables and implement policies to ensure that transient tables are properly deleted at regular intervals.

If you also want to keep a backup of data, such as IOC.CAPALERT, you can do so by backing up the IOC.CAPALERT tables and removing any duplicates. Section 4.3, “Backing up and restoring” on page 90 has information about how to back up and recover data.

Attention: It is important to back up the data before pruning the database. If you are running a backup of the database tables for the first time, verify that the backup process completes correctly.

The database tables to prune include the following tables:

- ▶ IOC.CAPALERT
- ▶ IOC.CAPINFO
- ▶ IOC.NOTIFICATION
- ▶ IOC.COMMON.EVENT

These tables can be pruned automatically by running scripts. The snippets that are shown in Example 4-5 can be used to generate a script that prunes the database tables.

Example 4-5 Script snippet of a basic connection to a database instance

```
echo "Starting pruning IOC database tables CAPALERT, CAPINFO, and EVENT ..."
db2 "connect to IOCDDB user db2inst1 using db2inst1" 2>&1
```

The snippet in Example 4-6 describes how to prune the IOC.COMMON.EVENT data table where the message types are Cancel, the sender is the Infrastructure Publisher, and the message was sent over 14 days ago.

Example 4-6 Script snippet to prune the IOC_COMMON.EVENT database table

```
db2 "delete from IOC_COMMON.EVENT where EXTERNALEVENTID IN (SELECT CAPALERTID from
IOC.CAPALERT where (MSGTYPE = 'Cancel') OR ((SENT < CURRENT TIMESTAMP - 14 DAYS)
AND (SENDER <> 'Infrastructure Publisher')))" 2>&1
```

The script snippet in Example 4-7 shows how to prune the IOC.CAPALERT table where the message types are Cancel, the sender is the Infrastructure Publisher, and the messages were sent more than 14 days ago. When an IOC.CAPALERT record is deleted, so is the corresponding IOC.CAPINFO record.

Example 4-7 Script snippet to prune IOC.CAPALERT

```
db2 "delete from IOC.CAPALERT where (MSGTYPE = 'Cancel') OR ((SENT < CURRENT
TIMESTAMP - 14 DAYS) AND (SENDER <> 'Infrastructure Publisher'))" 2>&1
```

The script snippet in Example 4-8 illustrates how to prune the notification data that was already been acknowledged or if the notification is over 14 days old.

Example 4-8 Script snippet to prune IOC.NOTIFICATION

```
db2 "delete from IOC.NOTIFICATION where (ACKNOWLEDGEDBY IS NOT NULL) OR
(SENTTIMESTAMP < CURRENT TIMESTAMP - 14 DAYS)" 2>&1
```

Procedures to back up and prune databases or other content should run regularly. Table 4-2 provides a sample policy that describes the type, frequency, and time window for backups. Included is a description that specifies how much data is backed up when the policy is run.

Table 4-2 Sample backup policy

Backup type	Frequency	Backup window	Amount of backup data received
Full	Monthly	00:00 - 03:00, first day of the month	12 months
	Weekly	00:00 - 03:00, Monday	5 weeks
Incremental	Daily	00:00 - 01:00	7 days

4.3 Backing up and restoring

There are several ways and strategies to back up the IBM Intelligent Operations Center environment.

To prevent the loss of valuable data in IBM Intelligent Operations Center, back up certain files, directories, and databases at regular intervals. When you extend IBM Intelligent Operations Center, it is a preferred practice to develop a backup procedure for the items you added, for example:

- ▶ Reports
- ▶ Ancillary databases
- ▶ Database tables
- ▶ Custom analytics
- ▶ Portlets
- ▶ Java applications

Also, consider data that you accumulated, for example:

- ▶ Common Access Protocol (CAP) database data
- ▶ IBM WebSphere Business Monitor database data
- ▶ Lightweight Directory Access Protocol (LDAP) user registry data (See 5.4, “Directory server backup and restore” on page 130.)
- ▶ Geographical Information System (GIS) data

This section describes a simple way to back up the IBM Intelligent Operations Center databases and the entire environment for the solution.

4.3.1 Backing up databases

Table 4-3 lists the databases that are on the data server that you should back up in IBM Intelligent Operations Center.

Table 4-3 IBM Intelligent Operations Center databases on the data server to backup

Service or component	Database instance	Database name
Intelligent Operations Center database	db2inst1	▶ IOcdb
Portal	db2inst2	▶ CUSTDB ▶ FDBKDB ▶ LKMddb ▶ JCRDB ▶ COMMdb ▶ RELDB
Business intelligence	db2inst3	▶ CXLOGDB ▶ CXCONTDB
Business rule and business activity monitor	db2inst4	▶ UDDIDB ▶ WODMDCDB ▶ MONITOR ▶ WBMdb ▶ RESDB
Semantic model	db2inst5	▶ JTS ▶ IIC

Service or component	Database instance	Database name
Service request management	db2inst6	▶ MAXIMO
Identity management	db2inst7	▶ TIMDB
Applications	db2inst8	▶ LDAPDB ▶ LDAPDB2B

The following commands describe the steps to back up and restore specific databases. Table 4-4 provides a definition of the query commands that are used in the steps.

Table 4-4 Description of query commands

Query command	Query description
CONNECT TO <DATABASE NAME>	Opens the connection with the database.
IMMEDIATE	Do not wait for the transactions to be committed; immediately roll back the transactions.
FORCE CONNECTIONS	Forces the connections off.
QUIESCE DATABASE	Forces all users off the specified instance and database and puts it into a quiesced mode. In quiesced mode, users cannot connect from outside of the database engine.
UNQUIESCE DATABASE	Restores user access to all objects in the quiesced database.
CONNECT RESET	Disconnects the current connection.
RESTORE DATABASE	Performs a database restore.
WITH num-buffers BUFFERS	The number of buffers to be used. DB2 automatically chooses an optimal value for this parameter unless you explicitly enter a value.
BUFFER buffer-size	The size, in 4 KB pages, of the buffer that is used when you build the backup image. DB2 automatically chooses an optimal value for this parameter unless you explicitly enter a value. The minimum value for this parameter is eight pages.
PARALLELISM n	Determines the number of table spaces that can be read in parallel by the backup utility. DB2 automatically chooses an optimal value for this parameter unless you explicitly enter a value.
WITHOUT PROMPTING	Specifies that the backup runs unattended, and that any actions that normally require user intervention return an error message.

To back up a specific database, run the following commands:

```
$ db2 CONNECT TO <DATABASE NAME>;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE <DATABASE NAME> TO "<DESTINATION DIRECTORY>" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO <DATABASE NAME>;
```

```
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

To restore a specific database, run the following commands:

```
$ db2 CONNECT TO <DATABASE NAME>;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 RESTORE DATABASE <DATABASE NAME> FROM "<SOURCE DIRECTORY>" TAKEN AT  
20120718201254 WITH num-buffers BUFFERS BUFFER 1024 PARALLELISM 1 WITHOUT  
PROMPTING;  
$ db2 CONNECT TO <DATABASE NAME>;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

Here are sample scripts that are used to back up each of the IBM Intelligent Operations Center database instances that are described in Table 4-2 on page 89:

► Instance 1 - IBM Intelligent Operations Center database

```
$ su - db2inst1  
$ mkdir backupdb # if does not exists  
  
$ db2 CONNECT TO IOADB;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE IOADB TO "/datahome/db2inst1/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO IOADB;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

► Instance 2 - Portal

```
$ su - db2inst2  
$ mkdir backupdb # if does not exists  
  
$ db2 CONNECT TO CUSTDB;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE CUSTDB TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO CUSTDB;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;  
  
$ db2 CONNECT TO FDBKDB;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE FDBKDB TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO FDBKDB;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;  
  
$ db2 CONNECT TO LKMDDb;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;
```

```
$ db2 BACKUP DATABASE LKMDDb TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO LKMDDb;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
```

```
$ db2 CONNECT TO JCRDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE JCRDB TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO JCRDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
```

```
$ db2 CONNECT TO COMMDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE COMMDB TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO COMMDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
```

```
$ db2 CONNECT TO RELDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE RELDB TO "/datahome/db2inst2/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO RELDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
```

► Instance 3 - Business intelligence

```
$ su - db2inst3
$ mkdir backupdb # if does not exists
```

```
$ db2 CONNECT TO CXLOGDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE CXLOGDB TO "/datahome/db2inst3/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO CXLOGDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
```

```
$ db2 CONNECT TO CXCONTDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE CXCONTDB TO "/datahome/db2inst3/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO CXCONTDB;
```

```

$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
▶ Instance 4 - Business rule and business activity monitor
$ su - db2inst4
$ mkdir backupdb # if does not exists

$ db2 CONNECT TO UDDIDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE UDDIDB TO "/datahome/db2inst4/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO UDDIDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;

$ db2 CONNECT TO WODMDCDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE WODMDCDB TO "/datahome/db2inst4/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO WODMDCDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;

$ db2 CONNECT TO MONITOR;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE MONITOR TO "/datahome/db2inst4/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO MONITOR;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;

$ db2 CONNECT TO WBMDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE WBMDB TO "/datahome/db2inst4/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO WBMDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;

$ db2 CONNECT TO RESDB;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE RESDB TO "/datahome/db2inst4/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO RESDB;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;
▶ Instance 5 - Semantic model
$ su - db2inst5
$ mkdir backupdb # if does not exists

```

```
$ db2 CONNECT TO JTS;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE JTS TO "/datahome/db2inst5/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO JTS;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

```
$ db2 CONNECT TO IIC;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE IIC TO "/datahome/db2inst5/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO IIC;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

► Instance 6 - Service request management

```
$ su - db2inst6  
$ mkdir backupdb # if does not exists
```

```
$ db2 CONNECT TO MAXIMO;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE MAXIMO TO "/datahome/db2inst6/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO MAXIMO;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

► Instance 7 - Identity management

```
$ su - db2inst7  
$ mkdir backupdb # if does not exists
```

```
$ db2 CONNECT TO TIMDB;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE TIMDB TO "/datahome/db2inst7/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO TIMDB;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

► Instance 8 - dsrdbm01 - Directory

```
$ su - dsrdbm01  
$ mkdir backupdb # if does not exists
```

```
$ db2 CONNECT TO LDAPDB;  
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;  
$ db2 CONNECT RESET;  
$ db2 BACKUP DATABASE LDAPDB TO "/datahome/dsrdbm01/backupdb/" WITH 2 BUFFERS  
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;  
$ db2 CONNECT TO LDAPDB;  
$ db2 UNQUIESCE DATABASE;  
$ db2 CONNECT RESET;
```

```

$ db2 CONNECT TO LDAPDB2B;
$ db2 QUIESCE DATABASE IMMEDIATE FORCE CONNECTIONS;
$ db2 CONNECT RESET;
$ db2 BACKUP DATABASE LDAPDB2B TO "/datahome/dsrdbm01/backupdb/" WITH 2 BUFFERS
BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING;
$ db2 CONNECT TO LDAPDB2B;
$ db2 UNQUIESCE DATABASE;
$ db2 CONNECT RESET;

```

4.3.2 Virtual infrastructure snapshots

Most virtual infrastructures have a snapshot feature that preserves the state and data of your virtual environment at a specific point. Take a snapshot of your environment before you perform any significant changes.

There are many virtual infrastructure management tools available, most of which have their own implementation of a snapshot feature. It is important to become familiar with the specific requirements and instructions about how to correctly back up your virtual environment by carefully reading the instructions that are provided by the virtual infrastructure vendor. Section 4.4, “Testing and production environments” on page 96 provides a sample workflow of a procedure to back up the IBM Intelligent Operations Center environment.

4.4 Testing and production environments

This section describes a procedure to migrate features from a development or test environment into a production environment of the IBM Intelligent Operations Center. Figure 4-3 shows an example of a process to migrate features or change requests to a production environment. It is important to back up or capture a snapshot of the production environment before you apply any changes to it. Section 4.3.2, “Virtual infrastructure snapshots” on page 96 describes creating snapshots of your virtual environment.

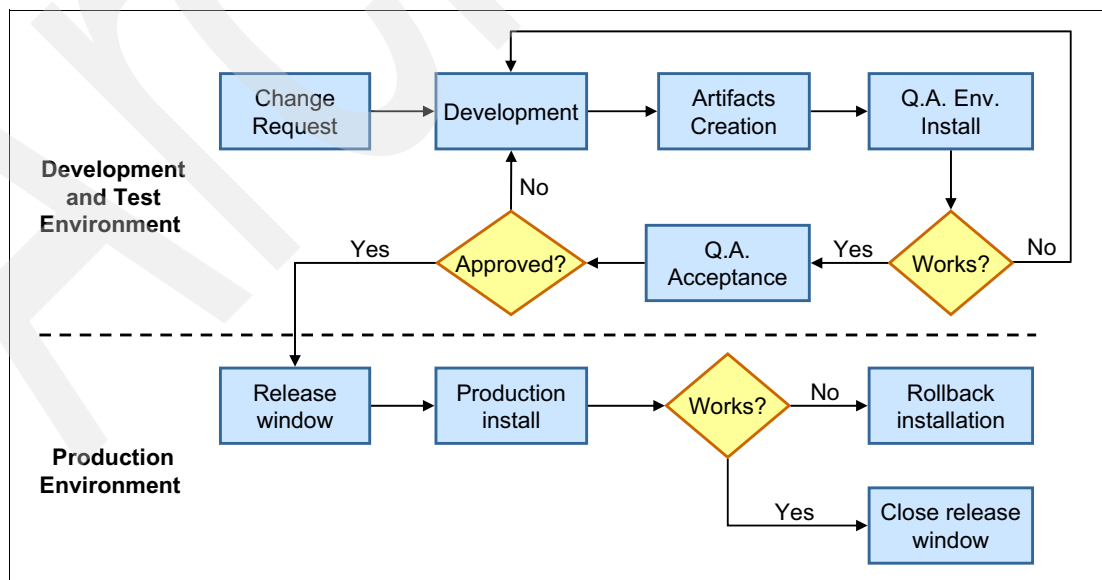


Figure 4-3 Migrating a feature or change request from development or test to production environment

The steps that are shown in Figure 4-3 on page 96 can be described as follows:

1. Change request: A feature or change is requested.
2. Development: The specialist or developer implements the feature on the development environment.
3. Artifacts creation: The specialist or developer documents the steps for both installation and removal of the feature and releases the installation package to the quality assurance team.
4. Q.A. env. install: The administrator follows the installation steps that are provided and runs the procedure on the test environment.
 - a. Q.A. acceptance: If the installation steps work, the administrator tests the uninstallation steps.
 - b. Q.A. rejection: If the installation steps do not work, the administrator documents the error and runs the uninstallation steps.
5. Release window: The administrator initiates the release window, which locks access for all users and takes a snapshot of the current production environment.
6. Production installation: The administrator runs the procedure on production environment.

Rollback installation - If the installation fails, the administrator documents the issue and runs the uninstallation process. If the uninstallation also fails, the snapshot of the production environment is reloaded.
7. Close the release window: The administrator unlocks access for all users.

4.5 Tivoli Enterprise Portal

Tivoli Enterprise Portal is a tool that provides useful information that is necessary to keep a healthy IBM Intelligent Operations Center running. This web-based console is also available offline as a Java based client. Its user interface presents various views and information about the IBM Intelligent Operations Center servers vital signs. You can start the Tivoli Enterprise Portal from the Administration Consoles portlet, as described in 3.5, “System monitoring” on page 65.

At the Administration Console portlet, select **Application Monitoring** from the Management Server group and click **IBM Tivoli Enterprise Portal Web Client** (Figure 4-4).



Figure 4-4 Tivoli Monitoring Service Index

After you log in to Tivoli Enterprise Portal, you see the workspace area. There are different views available from the workspace. Views are based on the Navigator view selection. The Navigator view is on the upper left of the workspace (Figure 4-5).

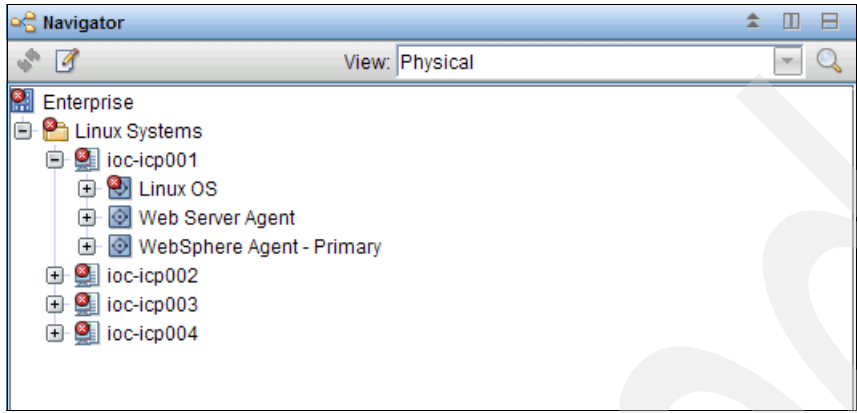


Figure 4-5 Tivoli Enterprise Portal navigator view

You can select a view from the Navigator View drop-down menu. The Physical view lists the IBM Intelligent Operations Center servers and solution components that run on each server. This visual representation of the resources helps pinpoint the source of the issues and monitors the health of the system.

Figure 4-6 shows the physical view of the Linux operating system that is running on one of the IBM Intelligent Operations Center servers.

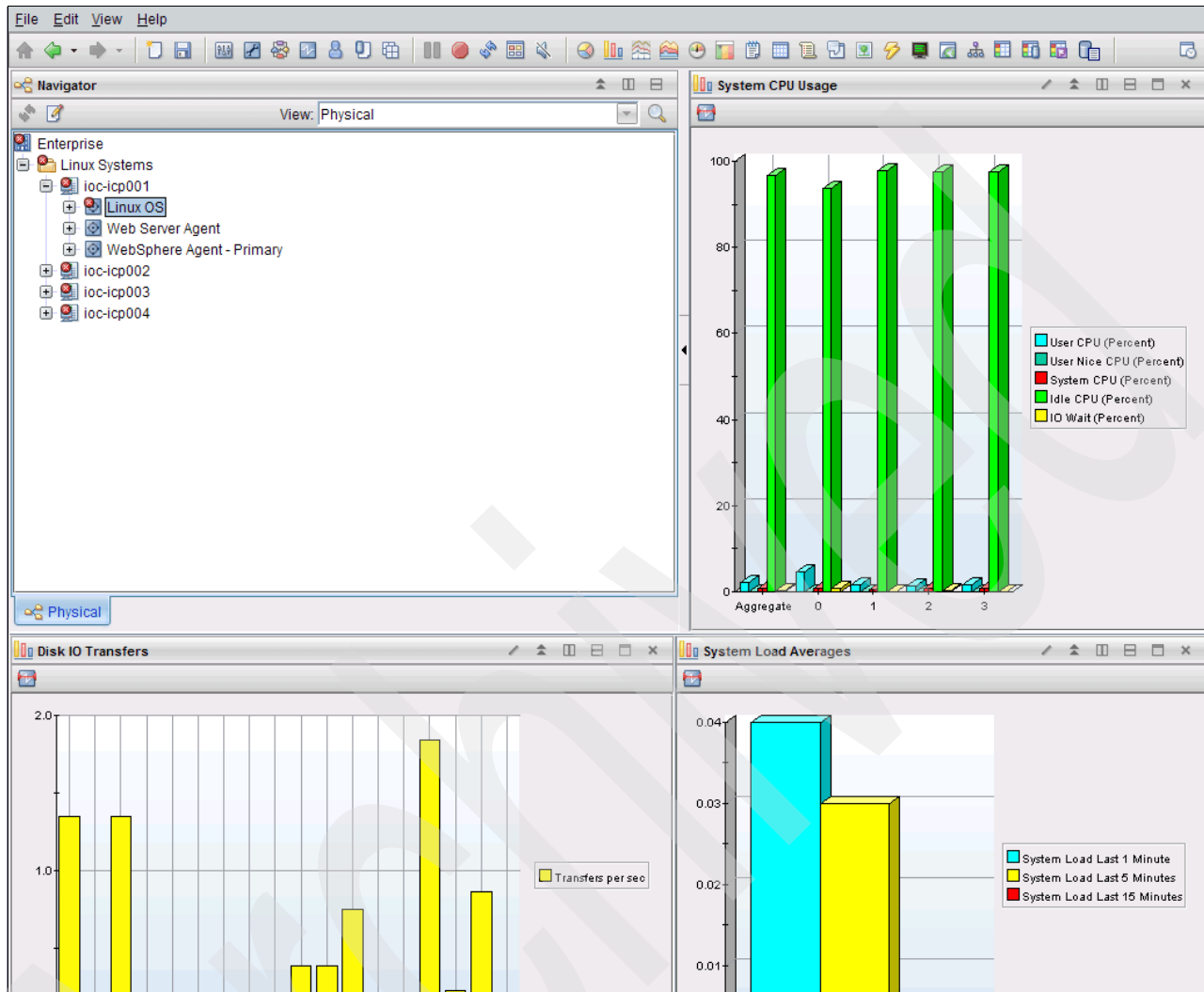


Figure 4-6 Tivoli Enterprise Portal physical view of Linux operating system

This view provides information about the health of the operating system. For example, processor usage, disk IO transfers, and system load averages.

For more information about using the Tivoli Enterprise Portal, see the IBM Tivoli Monitoring documentation at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=%2Fcom.ibm.itm.doc_6.2.2fp1%2Fwelcome.htm

For scenarios about using IBM Tivoli Monitoring, see *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443.

Archived

Security considerations

Securing the IBM Intelligent Operations Center solution is a critical part in production environments. This chapter provides information about security administration tasks that administrators must perform frequently and to make administrators aware of security configuration tasks that must be performed to secure the solution.

Topics that are covered in this chapter include:

- ▶ User IDs and password management
- ▶ Access control
- ▶ User management quick start scenarios
- ▶ Directory server backup and restore
- ▶ Single sign-on
- ▶ Troubleshooting security problems

For details about security configuration, customization, and guidelines, see the following resources:

- ▶ IBM Intelligent Operations Center Version 1.5 Information Center, found at:
<http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/ic-homepage.html>
- ▶ *IBM Intelligent Operations Center 1.5 Password Management Document*, found at:
<http://www.ibm.com/support/docview.wss?uid=swg21611122>

5.1 User IDs and password management

There are two kinds of user IDs and passwords that are related to IBM Intelligent Operations Center:

- ▶ Service user IDs and passwords

Service user IDs are used by IBM Intelligent Operations Center server components. The user names are set by the corresponding middleware components and the initial passwords are defined during the IBM Intelligent Operations Center solution installation.

- ▶ Solution user IDs and passwords

Solution user IDs are used by IBM Intelligent Operations Center users to log in to the IBM Intelligent Operations Center for business operations. These users passwords are set by the business users.

This section covers the following topics that are related to the service and solution user IDs:

- ▶ Service user IDs shipped with IBM Intelligent Operations Center
- ▶ Password management for service users
- ▶ Sample solution users shipped with IBM Intelligent Operations Center
- ▶ User policy settings for solution users
- ▶ User password policies
- ▶ Importing users from a user registry

5.1.1 Service user IDs shipped with IBM Intelligent Operations Center

All the user IDs for IBM Intelligent Operations Center components are created during the IBM Intelligent Operations Center installation and their passwords are set then. Some of the service components share user IDs in the user repository. Table 5-1 lists the service user IDs used by the IBM Intelligent Operations Center solution.

Table 5-1 Service user IDs in the IBM Intelligent Operations Center

User ID	Type	Description
root	OS	Operating system user ID.
dsrdbm01	OS	LDAP directory database. Directory server instance user.
cn=root	LDAP	LDAP administrator bind.
superadmin	LDAP	The LDAP administrator must configure the cn=root account. For the first login, the user ID = superadmin and password = secret.
tdsproxy	OS	LDAP proxy instance.
cn=root	LDAP	LDAP proxy administrator bind.
cn=bind	LDAP	LDAP proxy bind.
sec_master	TAM	Security service administrator. This user is granted privileges equivalent to the root user on the target servers. Because of the access this user has, make sure that the password is a long value, is different from other passwords, and is kept secure.
db2ibm	OS	Business activity monitoring service database.
db2wodm	OS	Decision management service database.
resAdmin1	LDAP	Decision management service administrator.

User ID	Type	Description
resDeployer1	LDAP	Decision management service rule deployer.
resMonitor1	LDAP	Decision management service monitor.
wodmdc	OS	Decision console database.
rtsAdmin	LDAP	Decision console administrator.
rtsConfig	LDAP	Decision console configuration.
rtsUser	LDAP	Decision console user.
db2uddi	OS	UDDI service database.
waswebadmin	LDAP	Application services administrator.
waswebadmin	LDAP	Administrator for the WebSphere Application Server console for the WebSphere Portal Server.
wpsadmin	LDAP	Administrator for the WebSphere Portal Server.
db2port1	OS	WebSphere Portal database.
Netcool	OS	Event service system administrator.
admin	Internal File Repository	Policy Service web administrator.
wasadmin	Internal File Repository	System event services administrator.
waswebadmin	LDAP	Service request manager administrator.
maximo	LDAP	Service request manager database.
maxadmin	LDAP	Service request manager administrator.
maxreg	LDAP	Service request manager user.
mxintadm	LDAP	Service request manager integration user.
waswebadmin	LDAP	Application services administrator.
itmuser	OS	Enterprise portal database.
waswebadmin	LDAP	Identity management administrator.
notes	OS	Collaboration system user.
IBM	N/A	Collaboration organization.
notes admin	LDAP	Collaboration administrator.
wpsadmin	LDAP	Collaboration portal administrator.
wpsbind	LDAP	Collaboration LDAP bind.
dasusr1 dasusr2 dasusr3 dasusr4 dasusr5 dasusr6 dasusr7 dasusr8	OS	Database services administrative server.
db2inst1	OS	Database services data server for IBM Intelligent Operations Center.

User ID	Type	Description
db2inst2	OS	Database services data server for WebSphere Portal Server.
db2inst3	OS	Database services data server for reporting service.
db2inst4	OS	Database services data server for KPI service.
db2inst5	OS	Database services data server for semantic model service.
db2inst6	OS	Database services data server for standard operating procedures administration.
db2inst7	OS	Database services data server for system management.
db2inst8	OS	Database services data server.
ihadmin	LDAP	HTTP server.
mqm	OS	Messaging services user.
mqmconn	OS	Messaging services connection.
taiuser	LDAP	Application services security.
sysadmin	ITM	System management administrator. <i>Restriction:</i> Password must be 15 characters or less.
ibmadmin	OS	System administration tools. This user is granted privileges equivalent to the root user on the target servers. The Platform Control Tool runs under this user name. Because of the access that this user has, make sure that this password has a long value, is different from other passwords, and it is kept secure.
ibmuser	OS	System general user.
sysadmin	ITM	Monitoring System Management administrator.

5.1.2 Password management for service users

The initial passwords for the service user IDs listed in Table 5-1 on page 102 are set during the IBM Intelligent Operations Center installation. The person that installs IBM Intelligent Operations Center must provide the service users' passwords to the administrator as part of the installation documentation.

Administrators are responsible for maintaining these passwords according to the security policy of their organization. The *IBM Intelligent Operations Center 1.5 Password Management Document* provides guidelines for maintaining these passwords. It can be found at:

<http://www.ibm.com/support/docview.wss?uid=swg2161122>

For more information about password management for service users, see the "Securing the solution" topic in the IBM Intelligent Operations Center Version 1.5 Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/sec_intro.html

5.1.3 Sample solution users shipped with IBM Intelligent Operations Center

Sample users are created during the deployment of the IBM Intelligent Operations Center. Generic sample users are defined with user role groups and corresponding access permissions. These sample users are defined as examples *only* and are listed in Table 5-2.

Table 5-2 Sample IBM Intelligent Operations Center solution users

Sample group	Sample members	Permission on portal pages
CityWideOperator	akelly and wpsadmin	Operator:Operations Operator:Reports Location Map
CityWideExecutive	tdelorne	Supervisor:Status
CityWideSupervisor	scollins and wpsadmin	Supervisor:Status Supervisor:Operations Supervisor:Reports Location Map

You can use the sample users to understand user roles and groups and as examples to define IBM Intelligent Operations Center users in your organization. Either change the default password of the sample users or delete them when you no longer need these users as examples.

Attention: Do not delete the wpsadmin user. It is not a sample user; it is the user ID for the WebSphere Portal administrator.

5.1.4 User policy settings for solution users

Table 5-3 lists the global user policy settings for the IBM Intelligent Operations Center business users.

Table 5-3 Default global user policy settings

Name	Value	Description
Max Login Failures	10	Maximum number of login failures before the account is no longer allowed to participate in the secure domain.
Disable Time Interval	180 (sec)	After the failed login count reaches Max Login Failures, the account is locked for Disable Time Interval seconds.
Minimum Password Length	8	Minimum number of characters that are required for the password.
Max Password Age	91 (days)	Maximum time a password can be used before it expires.
Minimum Password Alphas	4	Minimum number of alphabetic characters that are required in a password.
Minimum Password Non-Alphas	1	Minimum number of non-alphabetic characters that are required in a password.
Max Password Repeated Characters	2	Maximum number of repeated characters that are allowed in a password.

Name	Value	Description
Password Spaces Allowed	Unset	Determine whether spaces are allowed in passwords.
Max Concurrent Web Sessions	Unset	Maximum number of concurrent web sessions to allow.
Account Expiration Date	Unset	Date the account expires.
Time of Day Access	Unset	Time of day access policy.

You can change the default global user policy settings with the IBM Tivoli Access Manager for e-business Web Portal Manager. To access the Web Portal Manager from the IBM Intelligent Operations Center Administration Consoles (see 3.3, “Administration Consoles” on page 55), complete the following steps:

1. Log in to the IBM Intelligent Operations Center as administrator (wpsadmin).
2. Expand **Intelligent Operations** → **Administration Tools**.
3. Click **Administration Consoles**.
4. Click **Application Server for Management** (Figure 5-1).



Figure 5-1 Starting the web-based console for Tivoli Access Manager

5. On the Integrated Solutions Console, expand **Tivoli Access Manager** → **Web Portal Manager** → **Users** and click **Show Global User Policy** (see Figure 5-2).

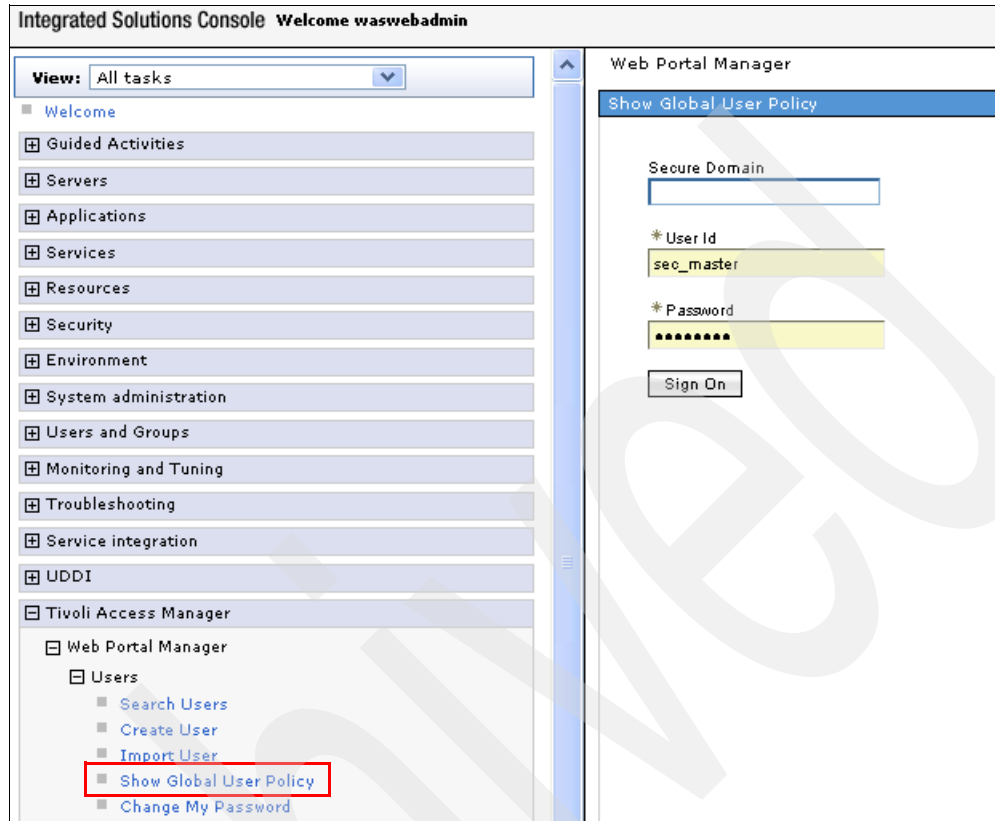


Figure 5-2 Logging in to the Web Portal Manager

6. Enter **sec_master** (security service administrator) in the user ID field and the corresponding password. Click **Sign On** (see Figure 5-2).
7. The Show Global User Policy page is displayed with the default values listed in Table 5-3 on page 105. Change the values for any of the policies on the Global User Policy page as required by the security policies of your organization (Figure 5-3 on page 108).

User Policy settings: You can change the user policy settings for specific users, such as password policies, login-failure policies, access policies, and account expiration policies with the IBM Tivoli Access Manager for e-business Web Portal Manager.

Web Portal Manager

Show Global User Policy

Max Login Failures

Unset

Set

Disable Time Interval

Unset

Disable

Set seconds

Minimum Password Length

Unset

Set

Max Password Age

Unset

Set Days Hours Mins Secs

Minimum Password Alphas

Unset

Set

Minimum Password Non-Alphas

Unset

Set

Max Password Repeated Characters

Unset

Set

Password Spaces Allowed

Unset

Yes

No

Max Concurrent Web Sessions

Unset

Displace

Unlimited

Set

Account Expiration Date

Unset

Unlimited

Set Month Day Year Hour Min Sec

Time of Day Access

Unset

Set Sunday Monday Tuesday Wednesday Thursday Friday Saturday

All Day

Between hours of: Start Time: End Time:

Local Time UTC Time

Figure 5-3 Changing the global user policy values

5.1.5 User password policies

You can enable enhanced password policies, for example, to ensure that users change their password after it is reset by the administrator. For more information about this subject, see the “Setting the global password policy” topic in the IBM Tivoli Directory Server Information Center at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd201.htm?path=8_4_4_8_1_9#wq589

For advanced password policy configuration, see *Tivoli Directory Server 6.1 password policy: enhancements, configuration, and troubleshooting* at:

<http://www.ibm.com/developerworks/tivoli/library/t-tdspp-ect/>

5.1.6 Importing users from a user registry

The process to add, manage, and delete the users that are described in this chapter assume that you use the IBM Intelligent Operations Center portal access links to manage user accounts. These links are the easiest way to manage user accounts.

However, in production environments, you might be required to manage user accounts through the organization’s user registry. The responsibility for managing the organization’s user registry lies with an LDAP administrator, who is not necessarily the same person that administers the IBM Intelligent Operations Center. In this case, to enable authentication and authorization by access management, all users that exist in a user registry must be imported, and you must make sure that a user of Tivoli Access Manager uses the Web Portal Manager or the `pdadmin` utility.

For information about importing users into IBM Tivoli Access Manager for e-business, see the “Importing users” topic in the IBM Tivoli Access Manager for e-business Information Center at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am611_admin271.htm?path=3_3_0_13_0_5#importusertask

5.2 Access control

There are three levels of access control and corresponding permissions that users need in IBM Intelligent Operations Center:

- ▶ Web resource permissions

These permissions provide coarse-grained access to web resources exposed by the IBM Intelligent Operations Center portal.

- ▶ Portal resource permissions

These permissions provide fine-grained access to the IBM Intelligent Operations Center portal resources.

- ▶ Data category permissions

These permissions provide access to a category of data (events, notifications, and KPIs) displayed in the IBM Intelligent Operations Center portlets.

Figure 5-4 shows an overview of access control in IBM Intelligent Operations Center.

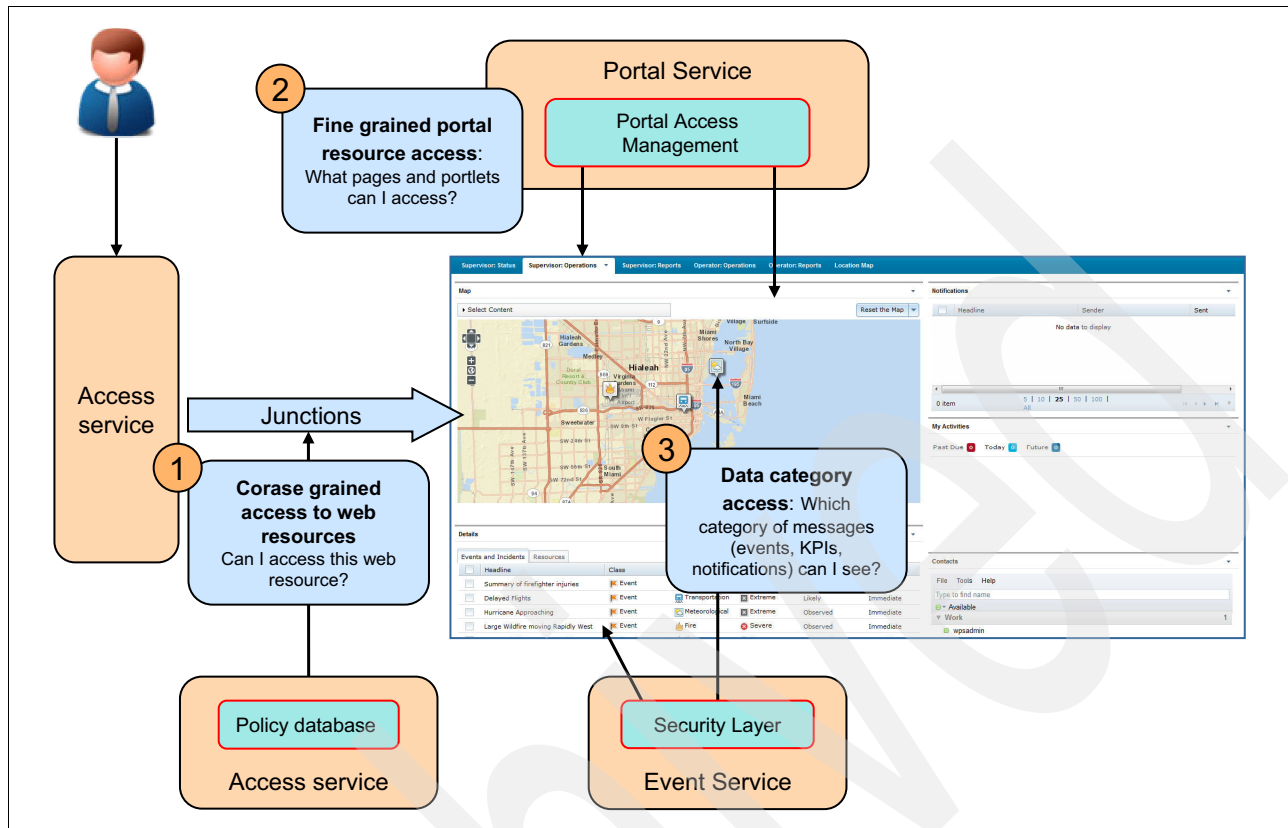


Figure 5-4 IBM Intelligent Operations Center access management overview

At the front end, access management services determine if a user can access a web resource that is based on the URL. For more information, see 5.2.1, “Web resource permissions” on page 110.

Based on their job responsibilities, IBM Intelligent Operations Center users need permissions to access:

- ▶ Portal resources (for example, pages and portlets)
- ▶ Category of data (for example, fire-related events, notifications, and KPIs)

The approach to give users the permissions they need is to add the users to two groups:

- ▶ User role group

A set of permissions to access portal resources is associated with a user role group. For more information, see 5.2.2, “Portal resource permissions and user role groups” on page 111.

- ▶ User category group

Permission to access a data category is associated with a user category group. For more information, see 5.2.3, “Data permissions and user category groups” on page 117.

5.2.1 Web resource permissions

Web resource permissions provide course-grained access to web resources exposed by the IBM Intelligent Operations Center portal. The web resources are represented by a URL.

A front-end Tivoli Access Management WebSEAL server protects web resources and applications on back-end web servers.

The connection between a WebSEAL server and a back-end web application server is known as a *WebSEAL junction*. A junction allows WebSEAL to provide protective services on behalf of the back-end server. WebSEAL can perform authentication and authorization checks on all requests before it passes those requests on to the back-end server.

As shown Table 5-4, there are six default predefined junctions in IBM Intelligent Operations Center.

Table 5-4 *WebSEAL junctions and the web services they protect*

Junction name	Target service
/wpsv70	Portal service
/stbaseapi	Collaboration service
/stwebapi	Collaboration service
/stwebclient	Collaboration service
/tsrm	Workflow service
/cognos	Reporting service

Administrators can add more junctions to link to other back-end services deployed in their environments. For more information, see the “Understanding WebSEAL junctions” topic in the IBM Tivoli Access Manager for e-business Information Center at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame2.doc_5.1/am51_webseal_guide16.htm

5.2.2 Portal resource permissions and user role groups

This section provides basic information about the permissions that users need to access portal resources.

Before you add users to the IBM Intelligent Operations Center environment, you should understand some of the basic concepts that are related to the permissions required by the users and how they obtain those permissions.

Customizing the portal environment: The customization of the portal environment for your organization, including resource access, is usually performed by experienced portal administrators and is beyond the scope of this book. The information in this section is provided as background information only. See the WebSphere Portal 8 product documentation for detailed information about portal security and access control at:

<http://www-10.lotus.com/ldd/portalwiki.nsf/xpViewCategories.xsp?lookupName=IBM%20WebSphere%20Portal%208%20Product%20Documentation>

Users need a set of permissions to access portal resources (for example, portal pages and portlets) in IBM Intelligent Operations Center based on their job role. A set of permissions is associated with a user role group. Administrators assign the required permissions to users by making them members of the appropriate group.

Before administrators can create users and add them to groups, the portal environment must be customized for the organization that is based on the different user job roles and their need to access portal resources. Pages on a portal are used to aggregate the portlets with the same role-specific tasks, so that users with specific roles can access the page and its portlets.

Portlets can be granted access permission on users or groups.

The wpsadmins group has an administrator role, which has permission to edit and configure portlets.

Table 5-5 shows the portal resources and user groups permissions that are shipped with IBM Intelligent Operations Center. The resources, groups, and permissions are different for each client environment after IBM Intelligent Operations Center customization.

Table 5-5 Sample portal resources and associated user role group permissions

Resource type	Resource name	City-wide Executive	City-wide Supervisor	City-wide Operator	wpsadmins
Page	Supervisor: Status	User permission	User permission	None	Administrator permission
	Supervisor: Operations	None	User permission	None	Administrator permission
	Supervisor: Reports	None	User permission	None	Administrator permission
	Operator: Operations	None	None	User permission	Administrator permission
	Operator: Reports	None	None	User permission	Administrator permission
	Location Map	None	User permission	User permission	Administrator permission
	Administration	None	None	None	Administrator permission

Resource type	Resource name	City-wide Executive	City-wide Supervisor	City-wide Operator	wpsadmins
Portlet	Status	User permission	User permission	None	Administrator permission
	Key Performance Indicator Drill Down	User permission	User permission	None	Administrator permission
	Notifications	User permission	User permission	User permission	Administrator permission
	Contacts	User permission	User permission	User permission	Administrator permission
	Map	User permission	None	User permission	Administrator permission
	Details	User permission	None	User permission	Administrator permission
	My Activities	User permission	User permission	User permission	Administrator permission
	Location Map	None	User permission	User permission	Administrator permission
	Reports	None	User permission	User permission	Administrator permission
	Intelligent Operations Center - About	None	None	None	Administrator permission
	Administration Consoles	None	None	None	Administrator permission
	System Verification Check	None	None	None	Administrator permission
	User Permissions Summary	None	None	None	Administrator permission
	Key Performance Indicators	None	None	None	Administrator permission
	Location Map Manager	None	None	None	Administrator permission
	Standard Operating Procedures	None	None	None	Administrator permission
	Event Scripting	None	None	None	Administrator permission
	Sample Publisher	None	None	None	Administrator permission
	User and Groups	None	None	None	Administrator permission

The user permission grants a user access to view and work with the page or portlet. The administrator permission grants an administrator access to:

- ▶ Configuring pages or portlets
- ▶ Creating, modifying, or deleting users and user groups

Checking user permissions: It is important for administrators to understand how to check user permissions to access portal resources. Lack of necessary permissions might be the reason why users cannot see a portlet on a page or data in a portlet.

For example, a user that is a member of the City-wide Supervisor group has permission to view and work with the following pages and portlets (see Table 5-5 on page 112):

- ▶ Pages:
 - Supervisor: Status
 - Supervisor: Operations
 - Supervisor: Reports
 - Location Map
- ▶ Portlets:
 - Status
 - Key Performance Indicator Drill Down
 - Notifications
 - Contacts
 - My Activities
 - Location Map
 - Reports

To view the environment that a user in the City-wide Supervisor group can view and work with, log in to the IBM Intelligent Operations Center as the sample user scollins.

Figure 5-5 shows the pages and portlets that the sample user Sue Collins can see, which matches the resource access for users in the CityWideSupervisor group.

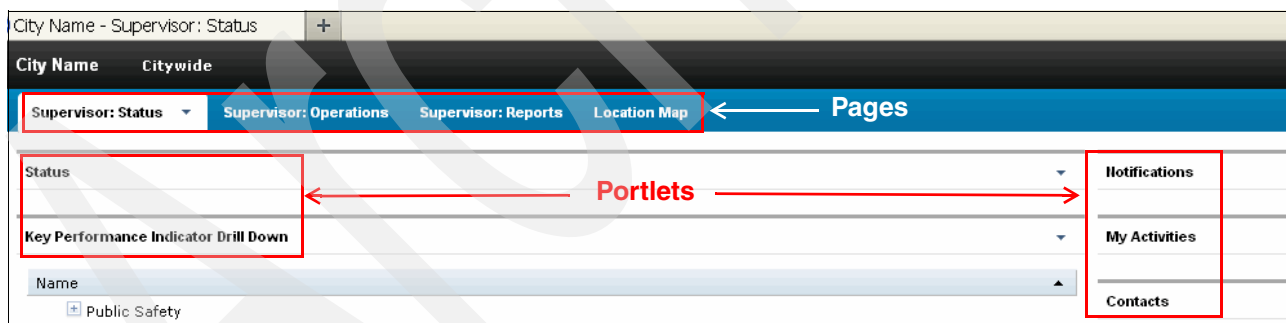


Figure 5-5 Portal view for a member of the CityWideSupervisor user group

Tip: For example, if a user in the CityWideSupervisor group reports that they cannot see the Map portlet that a user in the CityWideOperator group can see, that is because the Map portlet is on the Operator: Operations page. Users in the CityWideSupervisor group do not have access to the Operator: Operations page.

As an example, to check the resource permissions for the Operator: Operations page, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as wpsadmin.
2. Click **Administration** → **Access** → **Resource Permissions**.

3. On the Resource Permissions pane, click **Pages** under Resource Types (Figure 5-6).

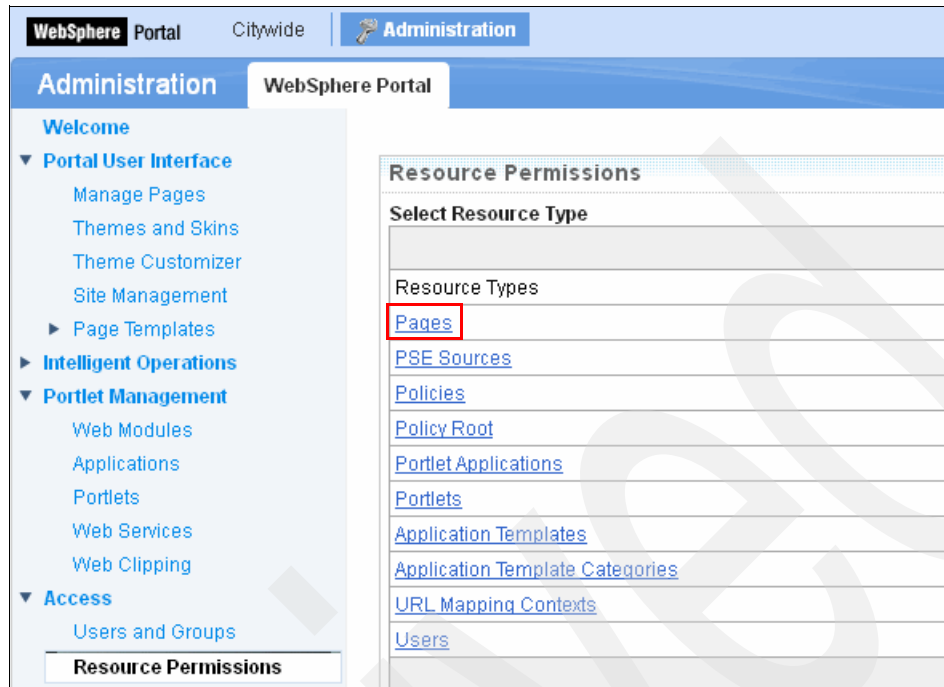


Figure 5-6 Checking portal pages permissions

4. Click **Root** → **Citywide** (Figure 5-7).

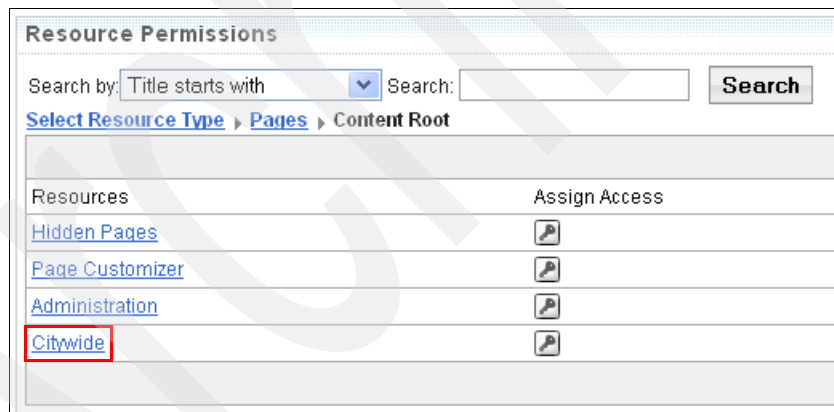


Figure 5-7 Resource permissions for Citywide portal pages

5. Enter Operator: in the Title starts with field and click **Search** (Figure 5-8).

Resource Permissions

Search by: Search:

[Select Resource Type](#) > [Pages](#) > [Content Root](#) > [Citywide](#)

Resources	Assign Access
Operator: Reports	
Operator: Operations	

Figure 5-8 Searching for the Operator:Operations page

6. Click the **Assign Access** icon for Operator:Operations to display user roles (Figure 5-8).
7. Click **Edit Role** by role type User to display users or groups that have user access to the Operator:Operations page (Figure 5-9).

Resource Permissions

[Select Resource Type](#) > [Pages](#) > [Content Root](#) > [Citywide](#) > [Operator: Operations](#)

Roles	Allow Propagation	Allow Inheritance	Edit Role
Administrator	✓	✓	
Security Administrator	✓	✓	
Markup Editor	✓	✓	
Manager	✓	✓	
Editor	✓	✓	
Privileged User	✓	✓	
User	✓	✓	

Figure 5-9 User access for Operator:Operations page (1 of 2)

8. As shown in Figure 5-10, you see that only the members of the CityWideOperator group have user access to the Operator:Operations page.

Resource Permissions

[Select Resource Type](#) > [Pages](#) > [Content Root](#) > [Citywide](#) > [Operator: Operations](#) > [User](#)

Members in the Role	Delete Member from Role
CityWideOperator	

Figure 5-10 User access for Operator:Operations page (2 of 2)

9. If you want users in other groups to have access to the Operator:Operations page, you can add user groups by clicking the **Add** button that is shown in Figure 5-10.

In summary, this example shows that users in the CityWideSupervisor group cannot see the Map portlet because this portlet is deployed on the Operator:Operations page and only users in the CityWideOperations group have user access to this page.

You can use this example to check resource permissions in your specific portal environment.

For detailed information about IBM Intelligent Operations Center resources and associated user role group permissions, see the “Securing the solution” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/sec_intro.html

5.2.3 Data permissions and user category groups

Permission to access a category of data in the IBM Intelligent Operations Center is associated with a *user category group*. The membership in a user category group determines the events, KPIs, and alert data that the user can see.

Example 5-1 shows a sample event with the event category value *Infra*. Such an event can be seen only by users that have permission to access *infrastructure* data.

Example 5-1 Event category example

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>fe83c2ee-3f37-4b02-98f8-d7ded1235e0e</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T15:41:16-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <restriction/>
  <code>Event</code>
  <info>
    <language>en_US</language>
    <category>Infra</category>
    <event>Water Main Break</event>
    <urgency>Expected</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <headline>Main water line break on 55th St.</headline>
    <description>Water line break on 55th street impacting citizen water
service.</description>
    <contact>{"telephone":"","name":"","email":""}</contact>
    <area>
      <circle>25.82511,-80.22866 0</circle>
    </area>
  </info>
</alert>
```

An administrator assigns data access to a user by making the user a member of the appropriate user category group. Each user is assigned membership in one or more user category groups.

Table 5-6 lists the data categories that are covered by the IBM Intelligent Operations Center and the corresponding user category groups that are used to identify event, KPIs, and alert data.

Table 5-6 User category group descriptions and identifiers

Data category	Description	User category groups	Sample users membership
CBRNE	Chemical, biological, radiological, nuclear, or high-yield explosive threat or attack	ioc_base_chemical	scollins, tdelorne, akelly, and wpsadmin
		ioc_base_biological	scollins, tdelorne, akelly, and wpsadmin
		ioc_base_radiological	scollins, tdelorne, akelly, and wpsadmin
		ioc_base_nuclear	scollins, tdelorne, akelly, and wpsadmin
		ioc_base_explosive	scollins, tdelorne, akelly, and wpsadmin
Env	Environment: pollution and other environmental	ioc_base_environmental	scollins, tdelorne, akelly, and wpsadmin
Fire	Fire suppression and rescue	ioc_base_fire	scollins, tdelorne, akelly, and wpsadmin
Geo	Geophysical (including landslide)	ioc_base_geophysical	scollins, tdelorne, akelly, and wpsadmin
Health	Medical and public health	ioc_base_health	scollins, tdelorne, akelly, and wpsadmin
Infra	Infrastructure: utility, telecommunication, and other non-transport infrastructure	ioc_base_infrastructure	scollins, tdelorne, akelly, and wpsadmin
Met	Meteorological (including flood)	ioc_base_meteorological	scollins, tdelorne, akelly, and wpsadmin
Rescue	Rescue and recovery	ioc_base_rescue	scollins, tdelorne, akelly, and wpsadmin
Safety	General emergency and public safety	ioc_base_safety	scollins, tdelorne, akelly, and wpsadmin
Security	Law enforcement, military, homeland, and local/private security	ioc_base_security	scollins, tdelorne, akelly, and wpsadmin
Transport	Public and private transportation	ioc_base_transportation	scollins, tdelorne, akelly, and wpsadmin
Other	Other events, KPIs, or alerts	ioc_base_other	scollins, tdelorne, akelly, and wpsadmin

5.2.4 User permissions summary

The User Permissions Summary portlet displays the permissions that are associated with the IBM Intelligent Operations Center users and groups. The User Permissions Summary portlet displays details of group membership and permissions that are granted to users.

To access the User Permissions Summary portlet, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as administrator.
2. Click **Administration**.
3. Expand **Intelligent Operations** → **Administration Tools**.
4. Click **User Permissions Summary**.
5. On the User tab, enter the user ID of the user whose permissions you want to check and click **Submit** (Figure 5-11).

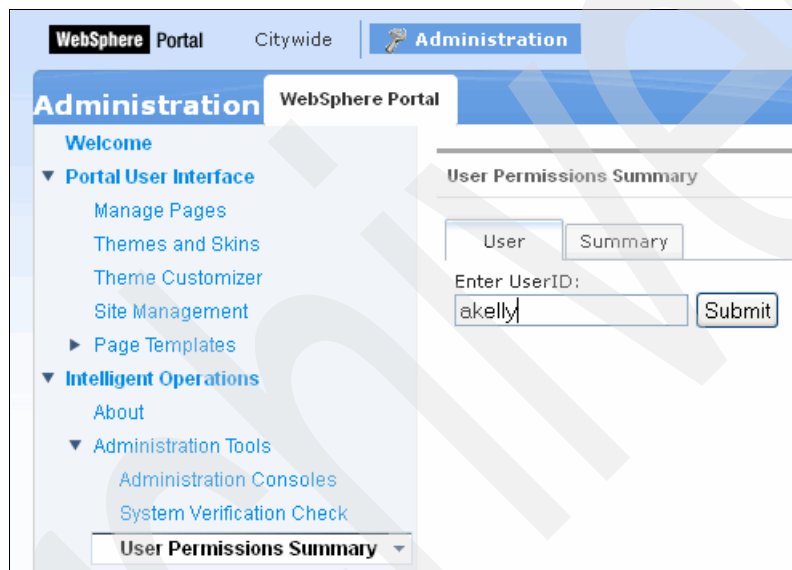


Figure 5-11 Checking user permissions

6. Figure 5-12 shows the results. The following information is displayed:
- A complete list of all the data categories and user category groups available in the IBM Intelligent Operations Center
 - A list of the data category permissions that are assigned to the specified user
 - A list of all the groups, user role groups, and user category groups, of which the specified user is a member
 - A list of each data category, which indicates whether the specified user has permission for that category

User Permissions Summary

Checking category permissions for user: akelly

Getting complete category permission list...
list is: {Other=[ioc_base_other], Security=[ioc_base_security], Infra=[ioc_base_infrastructure], Geo=[ioc_base_geophysical], Safety=[ioc_b

Getting user category permission list...
list is: [Infra, Security, Other, Geo, Safety, Rescue, Fire, Transport, CBRNE, Met, Health, Env]

Getting user groups list...
list is: [ioc_base_fire, CityWideOperator, ioc_base_other, ioc_base_health, ioc_base_security, ioc_base_biological, ioc_base_infrastructure, ioc

Checking each user category permission...

Permission for Other: true
Permission for Security: true
Permission for Infra: true
Permission for Geo: true
Permission for Safety: true
Permission for Rescue: true
Permission for Fire: true
Permission for Transport: true
Permission for CBRNE: true
Permission for Met: true
Permission for Health: true
Permission for Env: true

Checks Complete!

Enter UserID:

Figure 5-12 User Permissions Summary portlet - Users tab

7. Click the **Summary** tab to check summary statistics for users and group permissions (Figure 5-13). The following information is displayed:
 - Total number of groups in the IBM Intelligent Operations Center
 - Total number of users that are authorized to access the IBM Intelligent Operations Center
 - A list of the total number of users by data category
 - A list of the total number of users by user role group

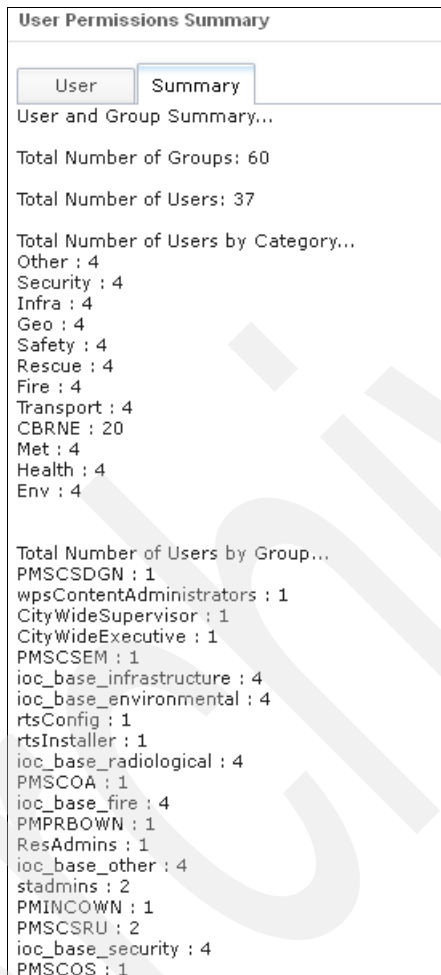


Figure 5-13 User Permissions Summary portlet - Summary tab

5.2.5 IBM Tivoli Directory Server Web Administration Tool

IBM Tivoli Directory Server Web Administration Tool is a web-based GUI used to manage the IBM Tivoli Directory Server. You must set up the Web Administration Tool before it can be used to manage the directory server. Complete the following steps:

1. Access the Tivoli Directory Server Web Administration Tool from IBM Intelligent Operations Center, as described in 3.3, "Administration Consoles" on page 55.

2. Click **Directory (Web-based console for Tivoli Directory Server)** (Figure 5-14).

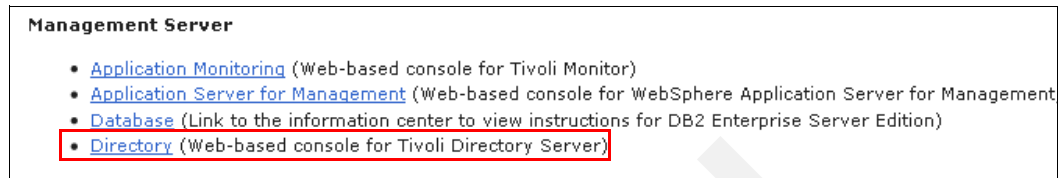


Figure 5-14 Starting the Tivoli Directory Server Web Administration Console

3. Log in to the console with the user ID of superadmin and password of secret (Figure 5-15).

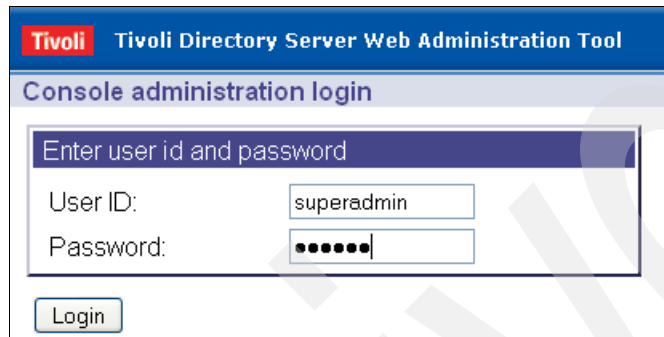


Figure 5-15 Logging in to the Tivoli Directory Server Console for the first time

4. Expand **Console administration** and click **Manage console servers**. Click **Add**.
5. Enter the host name for the IBM Intelligent Operations Center data server where the directory services are. Click **OK** (Figure 5-16).

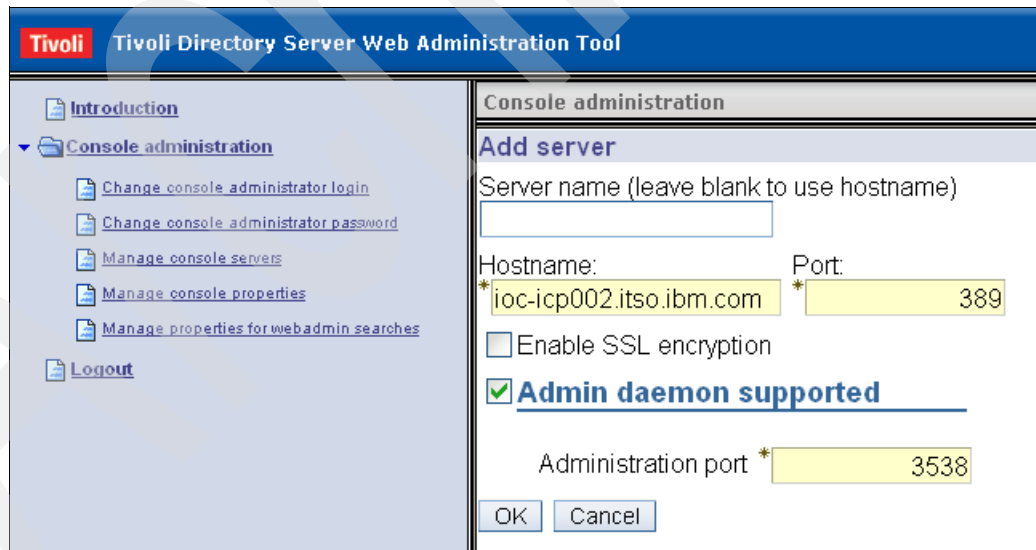


Figure 5-16 Setting up the Web Administration Tool to manage the directory server

6. Click **OK** for the message that confirms that the directory server was successfully added to the Web Administration Tool.
7. Click **Logout**.

8. The IBM Tivoli Directory Server Web Administration Tool is now configured to manage the directory server. You can log in to the console with User DN `cn=root` (Figure 5-17).

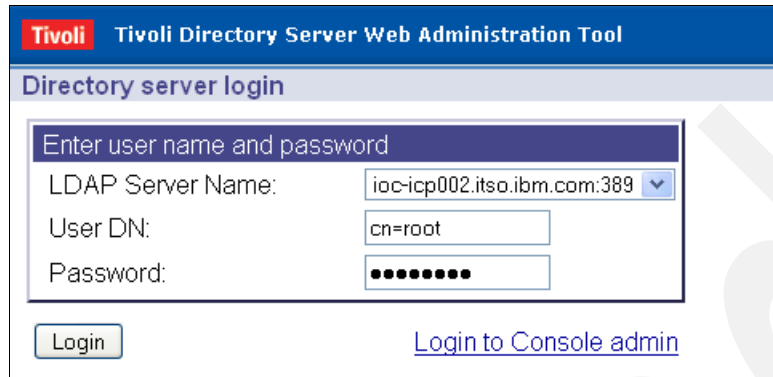


Figure 5-17 Directory server login

5.3 User management quick start scenarios

This section provides some simple examples to help you get started with the following scenarios:

- ▶ Adding a user with the operator role and permissions in order to view transportation data
- ▶ Checking user permissions
- ▶ Validating user permissions
- ▶ Changing a user's password
- ▶ Deleting a user

See the “Securing the solution” topic in the IBM Intelligent Operations Center Information Center for general information about the following subjects:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/sec_intro.html

- ▶ Adding a user or group
- ▶ Viewing or modifying group membership
- ▶ Viewing or editing a user profile
- ▶ Deleting a user or group
- ▶ Importing users and groups

User groups: The user role groups and the user category groups that are used in the examples in this section are the sample groups that are provided with IBM Intelligent Operations Center. The groups and the portal resources and category of data that they control vary for each customer environment.

5.3.1 Adding a user with the operator role and permissions in order to view transportation data

In this scenario, the administrator receives a service request to create a user with user ID *Mary*. Mary is an operator and needs access to transportation data. To add a user to satisfy this request, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as administrator (`wpsadmin`).
2. Click **Administration** → **Access** → **User and Groups**.

3. Click **New User** (Figure 5-18).

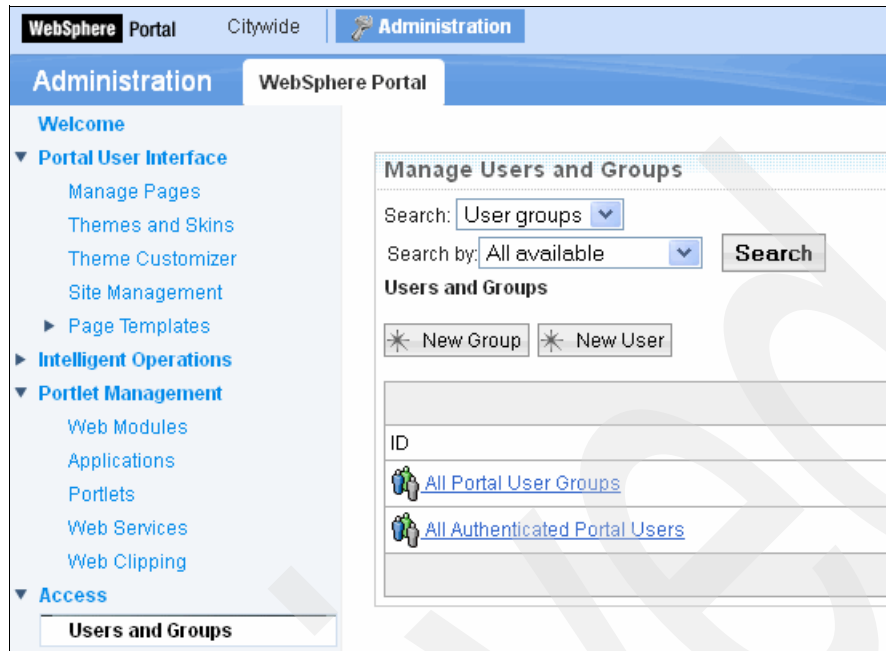


Figure 5-18 Adding a user

4. Enter the required information in the Profile Management portlet and click **OK**. The new user mary is created.

Now you must add Mary to the CityWideOperator user role group to grant Mary the permissions she needs to access the portal pages and portlets to do her job. For details about portal resources that can be accessed by members of the CityWideOperator group, see Table 5-5 on page 112.

To add the user mary to the CityWideOperator group, complete the following steps:

1. On the Manage Users and Groups portlet, select **cn** in the Search by drop-down menu, enter citywideoperator in the Search field, and click **Search** (Figure 5-19).

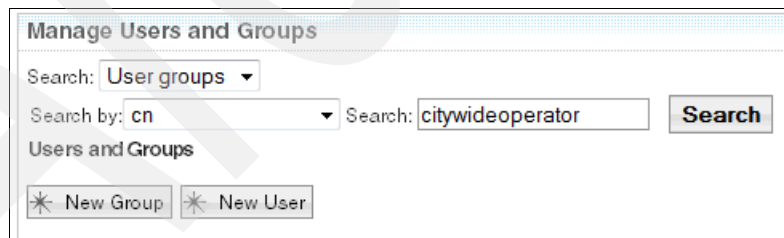


Figure 5-19 Searching for the citywideoperator group

2. In the results list, click **CityWideOperator**. The list of the members of this group is displayed.

3. Click **Add Member** (Figure 5-20).

Manage Users and Groups

Search: User groups ▾

Search by: All available ▾ **Search**

Users and Groups ▸ CityWideOperator

Members of cn=CityWideOperator,ou=GROUPS,ou=SWG,o=IBM,c=US - add

* New Group * New User * **Add Member**

ID
akelly

Figure 5-20 Adding a user to the CityWideOperator group

4. Advance through the pages by clicking the next page button until you find the user mary. Select the check box to select user mary and click **OK** (Figure 5-21).

Manage Users and Groups

Search: User groups ▾

Search by: All available ▾ **Search**

User groups whose name contains cn=CityWideOperator,ou=GROUPS,ou=SWG

<input type="checkbox"/>	Name
<input type="checkbox"/>	wpsbind
<input type="checkbox"/>	PMSELF8SERVUSR
<input type="checkbox"/>	PMUSRADMUSR
<input type="checkbox"/>	PMPRBANALUSR
<input checked="" type="checkbox"/>	mary
<input type="checkbox"/>	PMPRBMGRUSR
<input type="checkbox"/>	resMonitor1
<input type="checkbox"/>	PMUSRMGRUSR
<input type="checkbox"/>	wpsadmin
<input type="checkbox"/>	PMSCSDGNUSR

OK **Cancel**

Figure 5-21 Adding user mary to the CityWideOperator group

As shown in Figure 5-22, Mary is now a member of the CityWideOperator group.

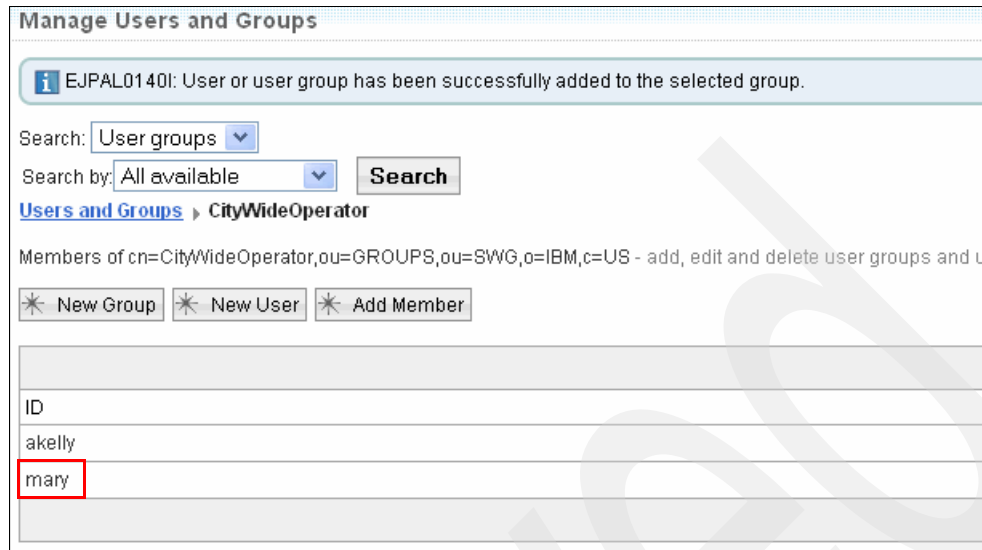


Figure 5-22 Mary is a member of the CityWideOperator user role group

5. Add Mary to the user category group that gives her permissions to view transportation data. According to Table 5-6 on page 118, the group is `ioc_base_transportation`. Repeat steps 1 on page 124 through 4 on page 125 to add mary to the `ioc_base_transportation` group (Figure 5-23).

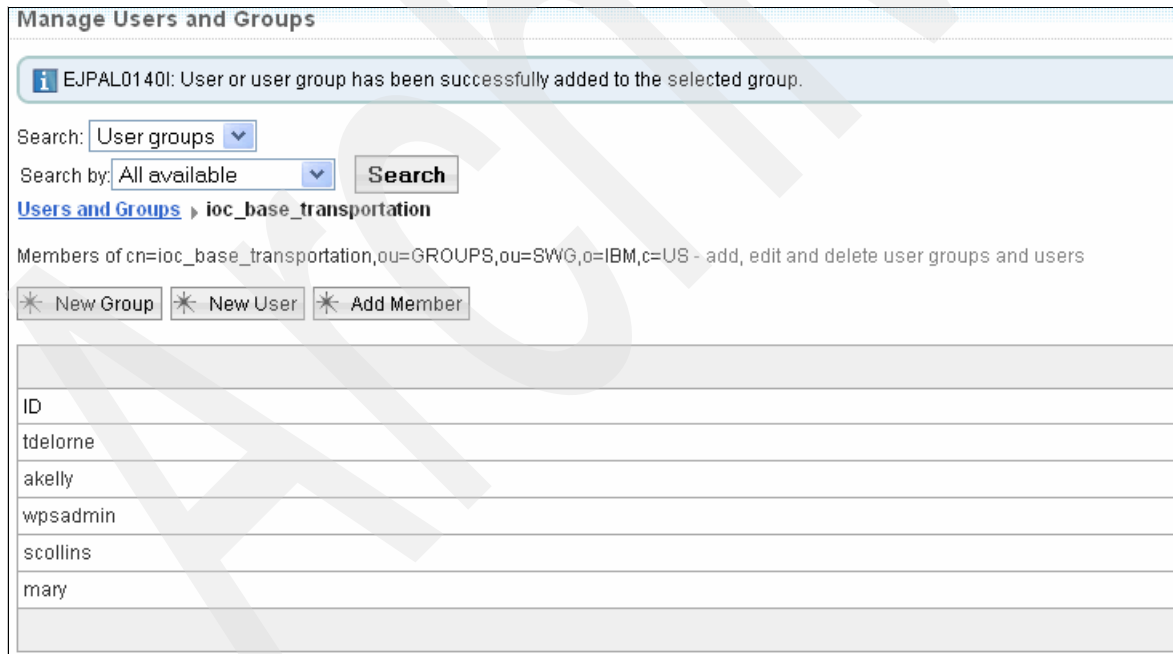
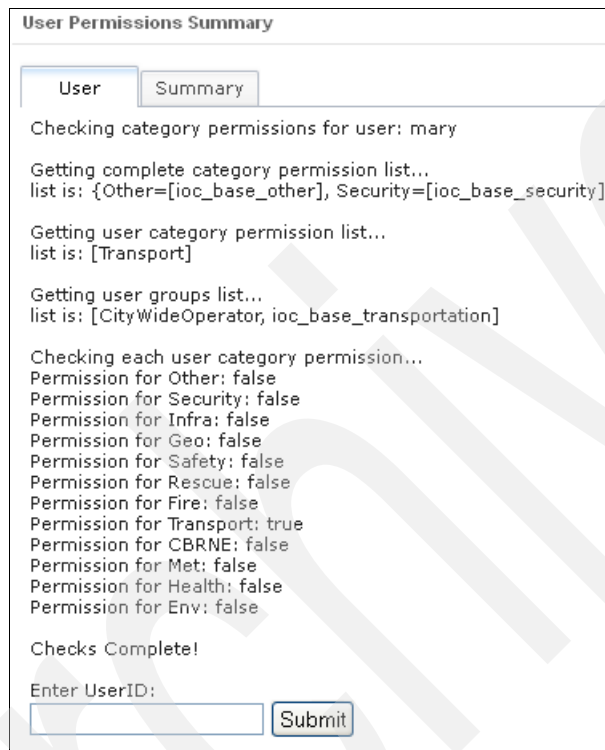


Figure 5-23 Mary is a member of the ioc_base_transportation data category group

5.3.2 Checking user permissions

Use the User Permissions Summary portlet to display the permissions that are associated with the user, as described in 5.2.4, “User permissions summary” on page 119. To check the permissions of user Mary created in 5.3.1, “Adding a user with the operator role and permissions in order to view transportation data” on page 123, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as administrator.
2. Click **Administration**.
3. Expand **Intelligent Operations** → **Administration Tools**.
4. Click **User Permissions Summary**.
5. In the User tab, enter the user ID mary and click **Submit**. Figure 5-24 shows the results.



The screenshot shows the 'User Permissions Summary' portlet interface. It has two tabs: 'User' (selected) and 'Summary'. The main content area displays the following text:

```
Checking category permissions for user: mary
Getting complete category permission list...
list is: {Other=[ioc_base_other], Security=[ioc_base_security],
Getting user category permission list...
list is: [Transport]
Getting user groups list...
list is: [CityWideOperator, ioc_base_transportation]
Checking each user category permission...
Permission for Other: false
Permission for Security: false
Permission for Infra: false
Permission for Geo: false
Permission for Safety: false
Permission for Rescue: false
Permission for Fire: false
Permission for Transport: true
Permission for CBRNE: false
Permission for Met: false
Permission for Health: false
Permission for Env: false
Checks Complete!
Enter UserID:
 Submit
```

Figure 5-24 User permissions summary for user mary

5.3.3 Validating user permissions

To ensure that Mary has the appropriate permissions for her job role, complete the following steps to validate her environment:


1. Log in to the IBM Intelligent Operations Center with user ID mary.
2. Check the following permissions for user mary:
 - **Page permission.** As a member of the CityWideOperator group, user mary can view the Operator:Operations, Operator:Reports, and Location Map pages (see Table 5-5 on page 112).
 - **Portlet permission.** As a member of the CityWideOperator group, user mary can view only the Key Performance Indicator Drill Down, Notifications, Contacts, Map, Details, My Activities, Location Map, and Reports portlets (see Table 5-5 on page 112).
 - **KPI permission.** As a member of the ioc_base_transportation category group, user mary can see only KPIs in the transportation category.

- **Event permission.** As a member of the ioc_base_transportation category group, user mary can see only Events in the transportation category.
- **Notification permission.** As a member of the ioc_base_transportation category group, user mary can see only Notifications in the transportation category.

5.3.4 Changing a user’s password

Users can change their own passwords and administrators can change passwords for users. If a user forgets their password, the administrator can change the password to a known value. The user can then change it to a value of their preference.

To change a user password as an administrator, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as the portal administrator (wpsadmin).
2. Click **Administration** → **Access** → **User and Groups**.
3. Click **All Authenticated Portal Users**.
4. In the Manage Users and Groups portlet, enter uid in the Search by field and enter mary in the Search field. Click **Search**.
5. Locate the user mary, and click the edit  icon (Figure 5-25).

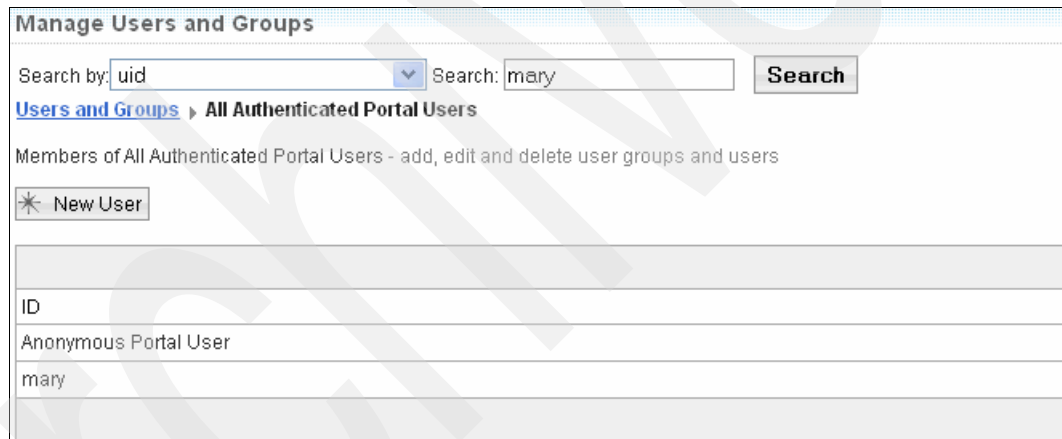
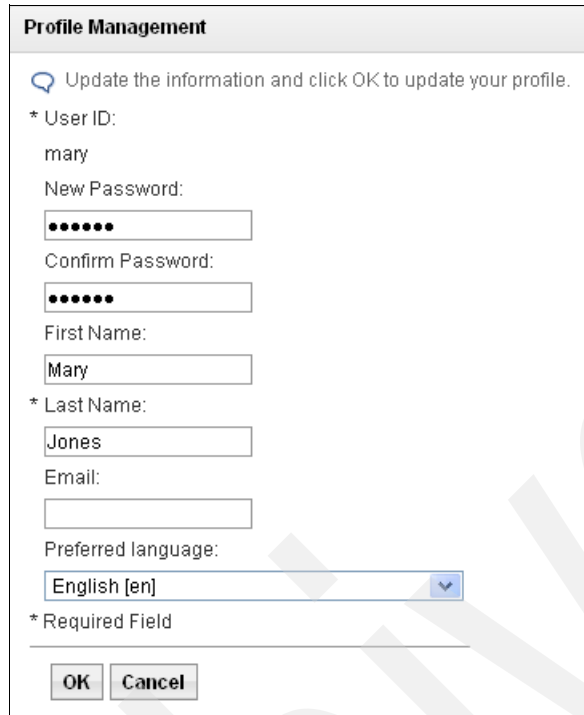


Figure 5-25 Editing a user profile

6. Enter the new password in the New Password and Confirm Password fields in the Profile Management portlet. Click **OK** (Figure 5-26).



The screenshot shows a 'Profile Management' dialog box with the following fields and values:

- User ID:** mary
- New Password:** [Redacted with dots]
- Confirm Password:** [Redacted with dots]
- First Name:** Mary
- Last Name:** Jones
- Email:** [Empty]
- Preferred language:** English [en]

Buttons for 'OK' and 'Cancel' are at the bottom.

Figure 5-26 Changing a user password

Users can change their own password by completing the following steps:

1. Log in to the IBM Intelligent Operations Center as a user, for example, mary.
2. Click **Edit My Profile** (Figure 5-27).

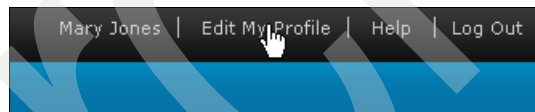



Figure 5-27 Editing a user profile

3. The Profile Management portlet that is shown in Figure 5-26 is displayed. The user can enter and confirm the new password.

5.3.5 Deleting a user

To delete a user, select the user from the list of authenticated portal users and delete it. To delete user mary, complete the following steps:

1. Log in to the IBM Intelligent Operations Center as the portal administrator (wpsadmin).
2. Click **Administration** → **Access** → **User and Groups**.
3. Click **All Authenticated Portal Users**.
4. In the Manage Users and Groups portlet, enter uid in the Search by field and enter mary in the Search field. Click **Search**.
5. Click the  **Delete** icon to delete user mary.

Attention: Do not delete required users. If you delete them, IBM Intelligent Operations Center does not operate correctly. For the full list of the required users, see the “Deleting sample users” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/install_delete_users.html

Deregistering users and groups

IBM WebSphere Portal stores users and groups that exist in the user registry as entries in the portal database. When you use the Manage User and Groups portlet to delete users and groups, they are deleted from the user registry and from the database. Deleting a user or group directly from the configured user registry does not remove the database entry.

For more information, see the “Deregistering users and groups” topic in the WebSphere Portal 8 product documentation at:

http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Deregistering_users_and_groups_wp8

5.4 Directory server backup and restore

There are several methods that you can use for backing up and restoring directory server instance information. There are methods that back up the complete information for a directory server instance (including configuration information), and methods that back up only the data in the database.

For detailed information and a description of the available backup and restore methods, see the “Directory server backup and restore” topic in the IBM Tivoli Directory Server Information Center at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd313.htm?path=8_4_4_12#backup_restore

You can choose to back up and restore only the directory server instance data that is stored in the DB2 database. This method backs up the DB2 data but not Tivoli Directory Server-specific configurations, such as the schema.

You can use the Tivoli Directory Server LDAP LDIF export and import commands, `idsdb2ldif` and `idsldif2db`, to export the data into an LDIF file and restore it from the LDIF file. For an example of exporting users, see 5.4.1, “Exporting LDAP users example” on page 130. For an example of exporting groups, see 5.4.2, “Exporting LDAP groups example” on page 131.

For more information about these commands, see the *IBM Tivoli Directory Server Version 6.3 Command Reference* at:

<http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/commandref.pdf>

5.4.1 Exporting LDAP users example

This example shows how to use the Tivoli Directory Server LDAP LDIF export command to dump user entries from the directory into a text file. This command can be run at any time; the server does not need to be stopped.

IBM Intelligent Operations Center user entries are in the following subtree:

ou=USERS,ou=SWG, o=IBM,c=US

To export the IBM Intelligent Operations Center user entries, complete the following steps:

1. Start a terminal session on the data server and log in as root.
2. Change to the directory /opt/ibm/ldap/V6.3/sbin.
3. Run the following command:

```
./db2ldif -I dsrdbm01 -o /tmp/exportUsers.ldif -s ou=users,ou=swg,o=ibm,c=us
```

Where:

- **dsrdbm01** is the directory service instance name.
- **/tmp/exportUsers.ldif** is the output LDIF file name and location.
- **ou=users,ou=swg,o=ibm,c=us** is the subtree distinguished name (DN) for users.

Example 5-2 shows the output of the command.

Example 5-2 Export users under subtree DN "ou=users,ou=swg,o=ibm,c=us"

```
[root@icp002 ~]# cd /opt/ibm/ldap/V6.3/sbin/
[root@icp002 sbin]# ./db2ldif -I dsrdbm01 -o /tmp/exportUsers.ldif -s
ou=users,ou=swg,o=ibm,c=us
GLPCTL113I Largest core file size creation limit for the process (in bytes):
'0'(Soft limit) and '-1'(Hard limit).
GLPCTL119I Maximum Data Segment(Kbytes) soft ulimit for the process is -1 and
the prescribed minimum is 262144.
GLPCTL119I Maximum File Size(512 bytes block) soft ulimit for the process is -1
and the prescribed minimum is 2097152.
GLPCTL122I Maximum Open Files soft ulimit for the process is 65536 and the
prescribed minimum is 4096.
GLPCTL122I Maximum Stack Size(Kbytes) soft ulimit for the process is 32768 and
the prescribed minimum is 10240.
GLPCTL119I Maximum Virtual Memory(Kbytes) soft ulimit for the process is -1 and
the prescribed minimum is 1048576.
GLPSRV200I Initializing primary database and its connections.
GLPD2L011I 44 entries have been successfully exported from the directory.
```

5.4.2 Exporting LDAP groups example

This example shows how to use the Tivoli Directory Server LDAP LDIF export command to dump group entries from the directory into a text file. This command can be run at any time; the server does not need to be stopped.

IBM Intelligent Operations Center user entries are in the following subtree:

ou=GROUPS,ou=SWG, o=IBM,c=US

To export the IBM Intelligent Operations Center group entries, complete the following steps:

1. Start a terminal session on the data server and log in as root.
2. Change to the directory /opt/ibm/ldap/V6.3/sbin.
3. Run the following command:

```
./db2ldif -I dsrdbm01 -o /tmp/exportGroup.ldif -s ou=groups,ou=swg,o=ibm,c=us
```

Where:

- **dsrdbm01** is the directory service instance name.
- **/tmp/exportGroups.ldif** is the output LDIF file name and location.
- **ou=groups,ou=swg,o=ibm,c=us** is the subtree distinguished name (DN) for groups.

Example 5-3 shows the output of the command.

Example 5-3 Export groups under subtree DN "ou=groups,ou=swg,o=ibm,c=us"

```
[root@icp002 ~]# cd /opt/ibm/ldap/V6.3/sbin/
[root@icp002 sbin]# ./db2ldif -I dsrdbm01 -o /tmp/exportGroup.ldif -s
ou=groups,ou=swg,o=ibm,c=us
GLPCTL113I Largest core file size creation limit for the process (in bytes):
'0'(Soft limit) and '-1'(Hard limit).
GLPCTL119I Maximum Data Segment(Kbytes) soft ulimit for the process is -1 and
the prescribed minimum is 262144.
GLPCTL119I Maximum File Size(512 bytes block) soft ulimit for the process is -1
and the prescribed minimum is 2097152.
GLPCTL122I Maximum Open Files soft ulimit for the process is 65536 and the
prescribed minimum is 4096.
GLPCTL122I Maximum Stack Size(Kbytes) soft ulimit for the process is 32768 and
the prescribed minimum is 10240.
GLPCTL119I Maximum Virtual Memory(Kbytes) soft ulimit for the process is -1 and
the prescribed minimum is 1048576.
GLPSRV200I Initializing primary database and its connections.
GLPD2L011I 61 entries have been successfully exported from the directory.
```

5.5 Single sign-on

IBM Intelligent Operations Center uses Tivoli Directory Server as its LDAP server to store user information. Single sign-on (SSO) is enabled for users to access the back-end web services through the IBM Intelligent Operations Center. As shown in Figure 2-2 on page 26, the security service for SSO is positioned as a protective front end to all services. It works as user login focal point in IBM Intelligent Operations Center to authenticate users and forward requests to the target services through the corresponding Tivoli Access Manager WebSEAL junction.

SSO between WebSphere Portal and the back-end servers uses an IBM Lightweight Third Party Authentication (LTPA) token to share user credentials. The common LTPA token that is shared across the back-end services is used by the junction to set up the trusted relationship with the target services. With this SSO approach, users can access back-end services without having to authenticate again.

Figure 5-28 shows the overview of SSO in the IBM Intelligent Operations Center.

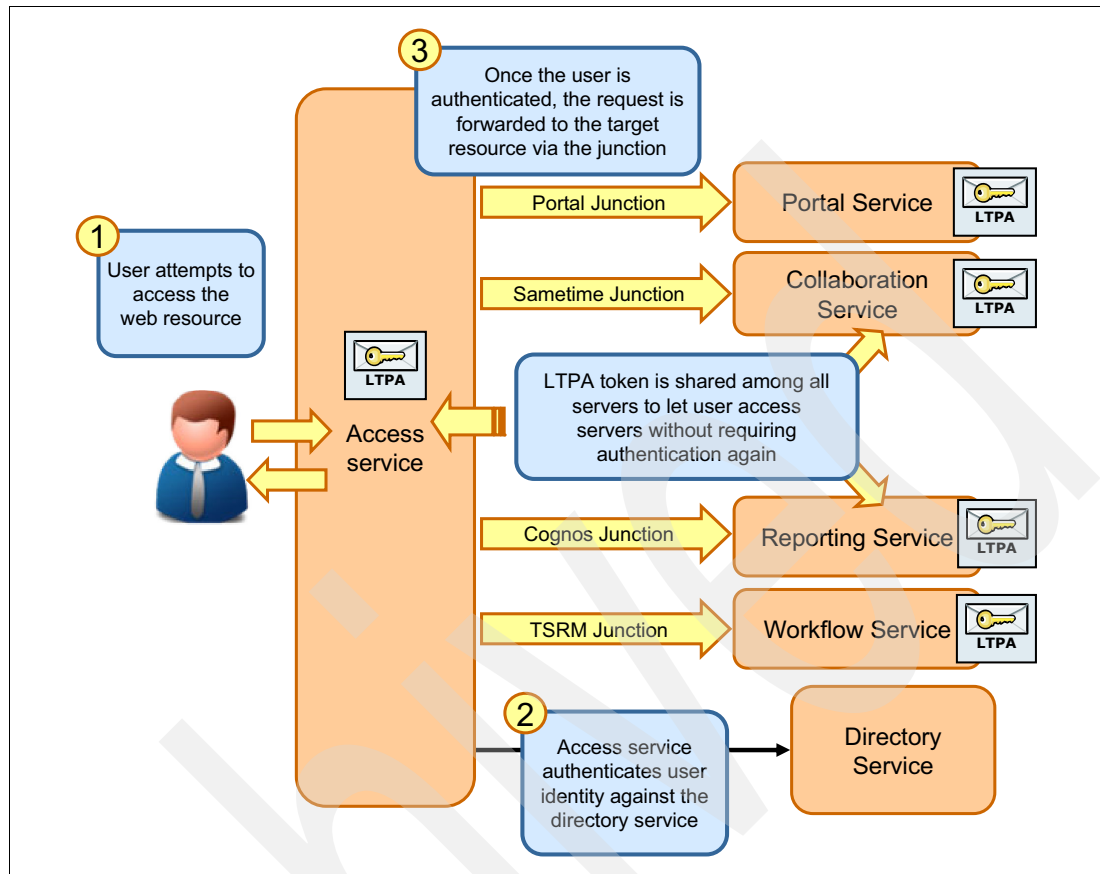


Figure 5-28 IBM Intelligent Operations Center single sign-on

5.5.1 Implementing SSO with a new back-end service

In the IBM Intelligent Operations Center solution, Tivoli Access Manager WebSEAL authenticates users when it accesses the IBM Intelligent Operations Center.

If there is a new application that is deployed on a back-end web application server, administrators can configure SSO. SSO within the IBM Intelligent Operations Center solution requires configuration in two areas:

- ▶ Configuring SSO between WebSphere Portal and the new web application that is deployed at the back end.
- ▶ Configuring SSO between Tivoli Access Manager WebSEAL and the new web application that is deployed at the back end.

The following steps provide an overview of the SSO configuration process:

1. Locate or export the portal LTPA key.

The default location of the LTPA key file is `/opt/pdweb/etc/portal.ltpa` on the application server node. If you cannot find this file, export the portal LTPA key. See the “Retrieving the WebSphere LTPA key” topic in the WebSphere Portal documentation, found at:

http://www-10.lotus.com/1dd/portalwiki.nsf/xpDocViewer.xsp?lookupName=IBM+WebSphere+Portal+7+Product+Documentation#action=openDocument&res_title=Retrieving_the_WebSphere_LTPA_key_for_use_with_Lotus_Domino_wp7&content=pdcontent

2. Import the LTPA key. Follow the appropriate procedure to import LTPA keys for the target application that is deployed.
3. Configure SSO between Tivoli Access Manager WebSEAL and the new web application by creating a Tivoli Access Manager WebSEAL junction with LTPA enabled by completing the following steps:

- a. Log in to the application server as user ID root.
- b. Log in to the Tivoli Access Manager WebSEAL `pdadmin` command console. Run the following command:

```
pdadmin -a sec_master -p password
```

- c. Run the following command to create the junction:

```
pdadmin> server task default-webseald-<server_name> create -t tcp -h  
<app_server_hostname> -p <app_server_port> -j -J trailer -A -2 -F  
<path_to_LTPA_key> -Z <LTPA_key_password> /<junction point>
```

Where:

- **default-webseald-<server_name>** is the fully qualified host name of the Tivoli Access Manager WebSEAL server. If you do not know the name, run `pdadmin -a sec_master -p <sec_master_password> server list` to find the server name.
- **-t tcp** is the TCP type of junction.
- **-h <app_server_hostname>** is host name of the back-end application server.
- **-p <app_server_port>** is the TCP port of the back-end application server. The default value is 80 for TCP junctions and 443 for SSL junctions.
- **-j** supplies junction identification in a cookie to handle script-generated server-relative URLs.
- **-J trailer** controls the junction cookie JavaScript block.
- **-A** enables or disables lightweight third-party authentication mechanism (LTPA) junctions. This option requires the **-F** and **-Z** options. The **-A**, **-F**, and **-Z** options all must be used together.
- **-2**, with the **-A** option, specifies that LTPA Version 2 cookies (LtpaToken2) are used.
- **-F /opt/pdweb/etc/portal.ltpa** specifies the location of the key file that is used to encrypt LTPA cookie data.
- **-Z <LTPA_password>** is the password of LTPA key to encrypt an LTPA cookie. It is valid only with **-A**.
- **/jctAppSvr** is a sample junction name.

For example:

```
pdadmin> server task default-webseald-icp004.itso.ibm.com create -t tcp -h  
icp004.itso.ibm.com -p 80 -j -J trailer -A -2 -F /opt/pdweb/etc/portal.ltpa -Z  
secret /jctAppSvr
```

For details about the `pdadmin` command `server task create`, see the IBM Tivoli Access Manager for e-business Information Center topic at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am611_cmdref134.htm?path=3_4_0_3_91#crejunct

5.6 Troubleshooting security problems

This section provides some guidelines about debugging and troubleshooting security problems.

5.6.1 Security logs

The logs for the main IBM Intelligent Operations Center security components are the starting point to troubleshoot security problems. Table 5-7 shows the location of the main security logs.

Tip: The logs in Table 5-7 grow without limits. Administrators must periodically archive the logs and free disk space, as described in 4.1.2, “Archiving log files” on page 86.

Table 5-7 Main IBM Intelligent Operations Center security logs

Security service	IBM Intelligent Operations Center server	Security component	Default location
Single sign-on	Application	WebSEAL	/var/pdweb/log/msg__webseald-default.log
Security	Management	Policy server	/var/PolicyDirector/log/msg__pdmgrd_utf8.log
		Authorization serve	/var/PolicyDirector/log/msg__pdacld_utf8.log

5.6.2 Tracing security components

If the information provided by the logs is not sufficient to determine the cause of the problem, you can enable trace for specific security components. Table 5-8 shows the main trace components for security in IBM Intelligent Operations Center.

Table 5-8 Trace components in IBM Intelligent Operations Center

Component	Description
pd.ivc.ira	The IRA is the Tivoli Access Manager interface in to the LDAP server. This trace component is used to trace the Tivoli Access Manager communication with the LDAP server.
pd.acl.authzn	Used to trace the authorization decision.
pdweb.debug	Used to trace the HTTP headers sent between WebSEAL and the client.

Component	Description
pdweb.snoop	Used to trace the HTTP packets that are transmitted between WebSEAL and the back-end server.
pdweb.wns.authn	Used to trace the authentication processing.
pdweb.wan.azn	Used to trace the WebSEAL authorization decision.
pdweb.wan.ltpa	Used to trace the management of LTPA cookies.

For information about the trace components, see *IBM Tivoli Access Manager for e-business Troubleshooting Guide* at:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am611_prob1em.htm

Trace level

The amount of detail in a trace component is controlled by the trace level. The trace level is a number 1 - 9, with 9 reporting the most amount of detail and 1 reporting the least amount of detail; 0 disables the trace of the component.

Enabling and disabling the trace

On the application server, run the `pdadmin` command `server task trace set` to enable or disable the gathering of trace information for the specified component and level. Here is the command syntax:

```
pdadmin -a sec_master -p <sec_master_password> server task
default-webseald-<server_name> trace set <component> <trace_level> file
path=<trace_file_path>
```

Where:

- <component>** Trace component name.
- <trace_level>** Reporting level. This required argument must be 1 - 9; 0 disables the trace.
- <trace_file_path>** The fully qualified name of the file to which trace data is written.

Attention: Use trace with caution, because it can severely degrade system performance. Before you enable trace in a production environment, enable and examine the trace in a test environment so that the administrator is aware of the possible effects of the trace before the production environment is affected.

Troubleshooting

This chapter explains how to identify and resolve some common problems you might experience when you use the IBM Intelligent Operations Center.

Topics that are covered in this chapter include:

- ▶ Section 6.1, “Troubleshooting scenarios” on page 138 provides detailed guidance and a checklist of things to consider during the resolution of many different troubleshooting scenarios. This section can be used with Chapter 7, “Data flows” on page 189, which gives details about the interconnection between the various subsystems of IBM Intelligent Operations Center.
- ▶ Section 6.2, “Troubleshooting resources and references” on page 187 provides information about various tools that are available from IBM to assist you with problem determination and reporting problems.

6.1 Troubleshooting scenarios

This section contains various troubleshooting scenarios and details about how to identify or resolve specific issues. Some of the scenarios provide step-by-step guidance to recover from the situation. The most important scenarios are associated with the data flows described in Chapter 7, “Data flows” on page 189.

Important: You must review 6.1.1, “Events that are not displayed in the Details portlet” on page 138 before you troubleshoot any of the other scenarios in this chapter. It provides a detailed overall connectivity of the internal systems that are similar to all the other data flow troubleshooting scenarios described in this chapter.

The following scenarios are covered in this section:

- ▶ Events that are not displayed in the Details portlet.
- ▶ Activities not displayed in the My Activities portlet.
- ▶ KPIs not displayed in the Status or Drill Down portlets.
- ▶ Notifications not displayed in portlet.
- ▶ Correlated notification not displayed.
- ▶ Resources are not being updated.
- ▶ Event Publisher tool not publishing events on the Details portlet.
- ▶ Unable to log in to the IBM Intelligent Operations Center.
- ▶ Login shows “Third-party server not responding” error message.
- ▶ Cannot access the login window.
- ▶ Portlets error “An error has occurred communicating with the servers”.
- ▶ User login expired error.
- ▶ Login shows the “Error 403: Authentication Failed” error.
- ▶ Portal shows the error message “There is no content available”.
- ▶ Portlets on the IBM Intelligent Operations Center page are closed.
- ▶ Contacts portlet prompts for user name and password.
- ▶ The Cognos Report page shows a server error.
- ▶ The KPI portlet is not refreshing the status.
- ▶ IBM Intelligent Operations Center page loads slowly.

The default pages and portlets (for example, Supervisor:Operations, Supervisor:Status, and Operator:Operations) shown in these troubleshooting scenarios are sample pages and portlets that are deployed with IBM Intelligent Operations Center. The sample pages and portlets are most likely renamed or removed in a production deployment of IBM Intelligent Operations Center.

Queue names: The queue names in the following sections are shortened to improve readability. Table 7-1 on page 189 shows the full and corresponding short queue names.

6.1.1 Events that are not displayed in the Details portlet

Event flow: The troubleshooting process that is described in this section is driven by the IBM Intelligent Operations Center event flow. For information about event flow, see 7.1, “Event flow” on page 190.

It is important to understand a basic event message. Example 6-1 shows a sample event in Common Alerting Protocol (CAP) format that is published to the IBM Intelligent Operations Center server. Notice the following items:

- ▶ The sent element is the current time stamp.
- ▶ The code element is set to Event in this example.
- ▶ The headline element value is displayed in the Details portlet and the Map portlet event icon.
- ▶ Values within the circle element provide the latitude and longitude position where the event occurred.

For more information about the CAP messaging protocol, see the *Oasis Common Alerting Protocol v.1.1* document at:

https://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf

Example 6-1 Sample event CAP formatted XML message

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>68cbe248-255e-4277-9e7b-67fe02096964</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T15:58:21-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <restriction/>
  <code>Event</code>
  <info>
    <language>en_US</language>
    <category>Transport</category>
    <event>Severe_Traffic_Accidents</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <headline>Multi Vehicle Accident with Injuries</headline>
    <description>Multi-vehicle accident with multiple injuries.</description>
    <area>
      <areaDesc>Palmetto Expressway West bound near RT 441.</areaDesc>
      <circle>25.92725,-80.21736 0</circle>
    </area>
  </info>
</alert>
```

IBM Intelligent Operations Center has five servers:

- ▶ Installation
- ▶ Application
- ▶ Database
- ▶ Event
- ▶ Management

For more information about these servers, see 2.1.1, “Servers overview” on page 24.

Use the following sections to diagnose event issues by logging in to the different servers with administration credentials and performing the steps that are described for each server.

Portal server: It is assumed in these steps the portal server is running and functional.

Application server

To diagnose event issues on the application server, complete the following steps:

1. Verify that all the services are running by using the System Verification Check tool. For more information about running System Verification Check tests, see 3.2, “System Verification Check” on page 48.
2. Verify that the user is authorized to access the Details portlet.

Figure 6-1 shows that the Map portlet is accessible, but the Details portlet that collects the events in tabular format does not show on the IBM Intelligent Operations Center Operator: Operations page.

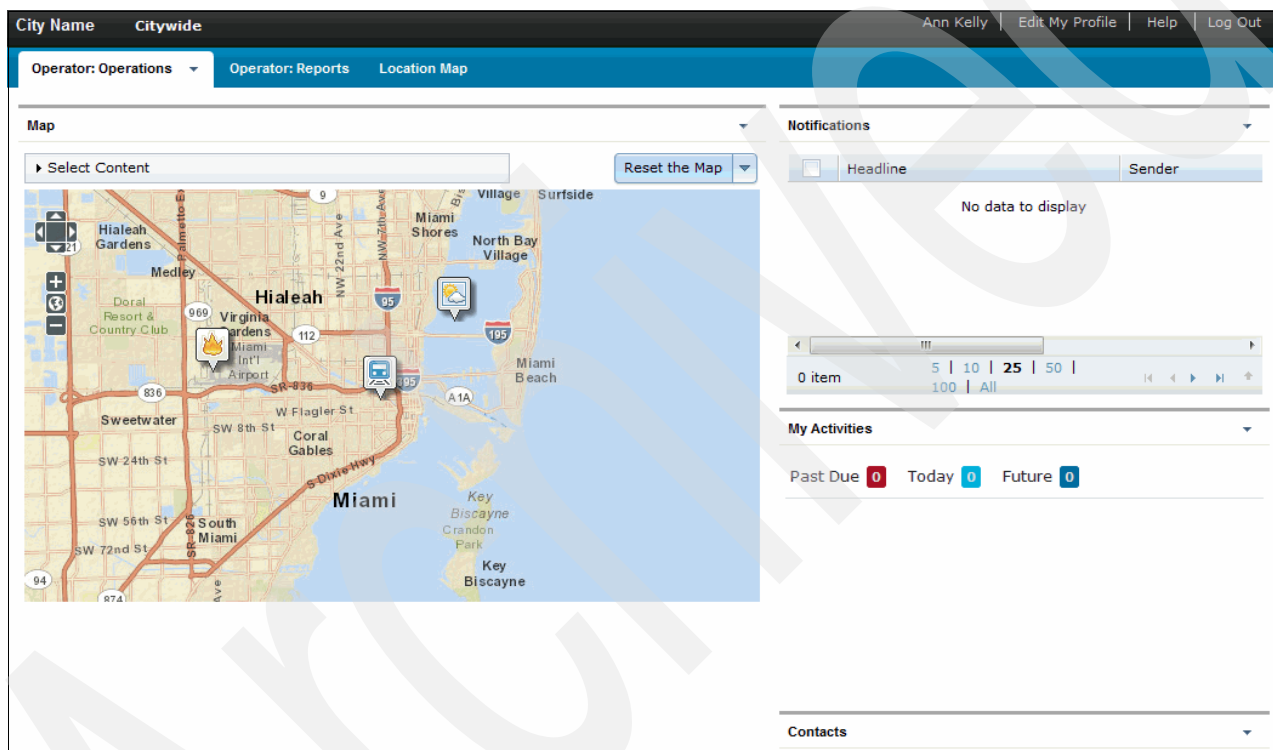


Figure 6-1 Details portlet not shown

Figure 6-2 shows there are no members with user role access to the Details portlet resource. To understand how permissions to portal pages and portlets are granted to users, see 5.2.2, “Portal resource permissions and user role groups” on page 111.

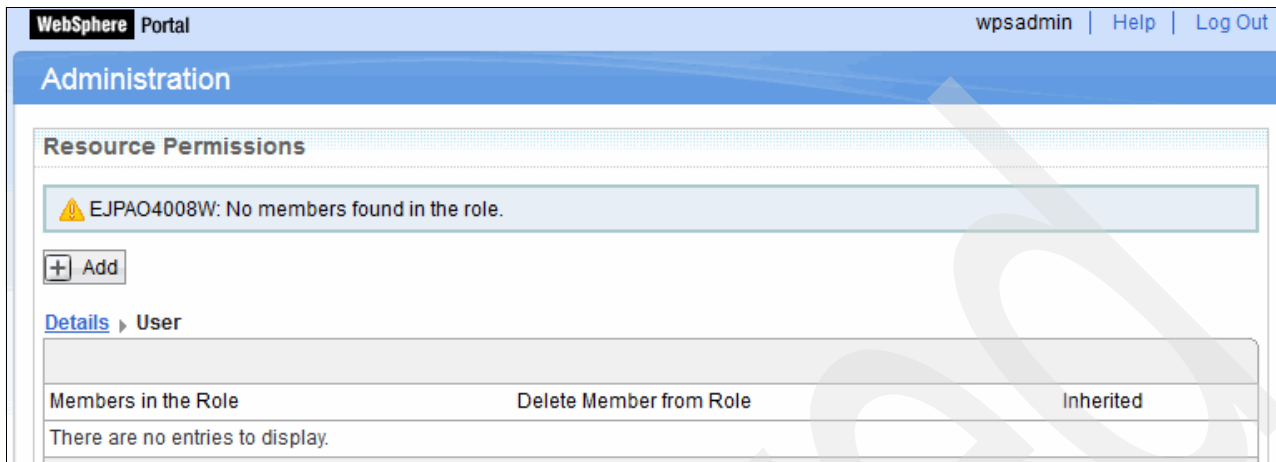


Figure 6-2 No members with a user role for portal resource - Details portlet

3. Ensure that the following portlet services are running:

- ioc_portal.ear
- iss_curi.ear
- iss_help.ear
- iss_portal.ear

To confirm that these portlet services are running, complete the following steps:

- a. Click **Administration Consoles** → **Application Server**, as described in 3.3, “Administration Consoles” on page 55.

- b. Log in to the application server with administration authority and click **Applications** → **Application Types** → **WebSphere enterprise applications**. Scroll down to see if the listed applications are running (Figure 6-3).

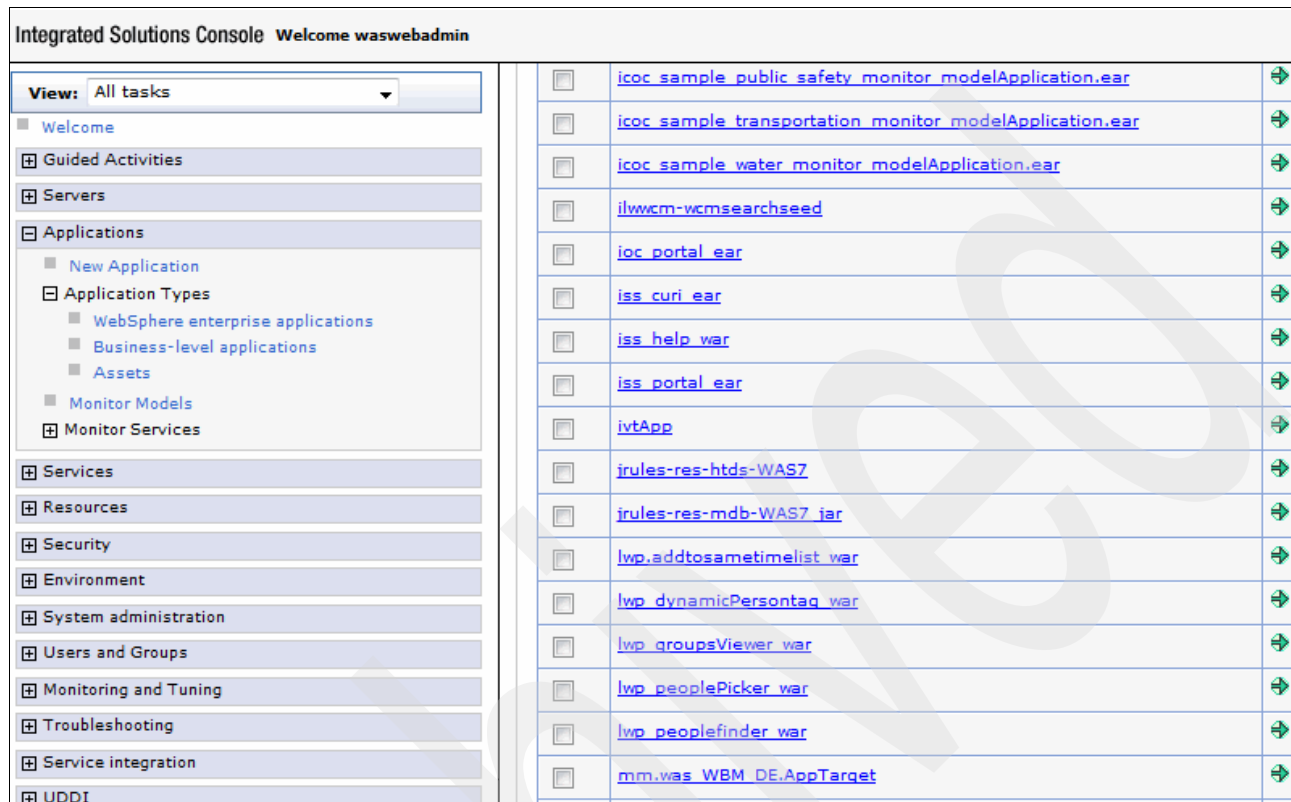


Figure 6-3 Map and portlet applications on the Administration console

4. Verify that the portlet is visible on the Supervisor:Operations or Operator:Operations portal page.
5. Go to the portlet **Details** → **Event and Incidents** tab and check if it is gathering other events. To verify, publish a test event with the Sample Event Publisher tool. For details, see 3.4, “Sample Event Publisher portlet” on page 59.
6. Verify that there are no errors in the portal logs for the event by checking the following logs in this application server:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Database server

To diagnose event issues on the database server, complete the following steps:

1. To verify that the database server is running, you can:
 - Run the System Verification Check tool, which shows the verification test results (Figure 6-4).



Figure 6-4 System Verification Check test for db2inst1 IOADB service status

- Run the following **IOControl** command to verify that the solution database is running:
`./IOControl.sh status db2sol <password>`

Example 6-2 shows the status of database service db2inst1 when it is stopped.

Example 6-2 Status for db2inst1 database

```

Executing stop command.....completed.
Executing query command...completed.
  IBM DB2 Enterprise server for Solution [ on ]
Command completed successfully.

```

2. Events are stored in the **IOC_COMMON.EVENT** and **IOC.CAPALERT** tables under the db2inst1 instance. To check these tables, complete the following steps:
 - a. Log in to the database server.
 - b. Run the following commands:


```

su - db2inst1
db2cc &

```
 - c. Select the **IOC.CAPALERT** table, as shown in Figure 6-5.

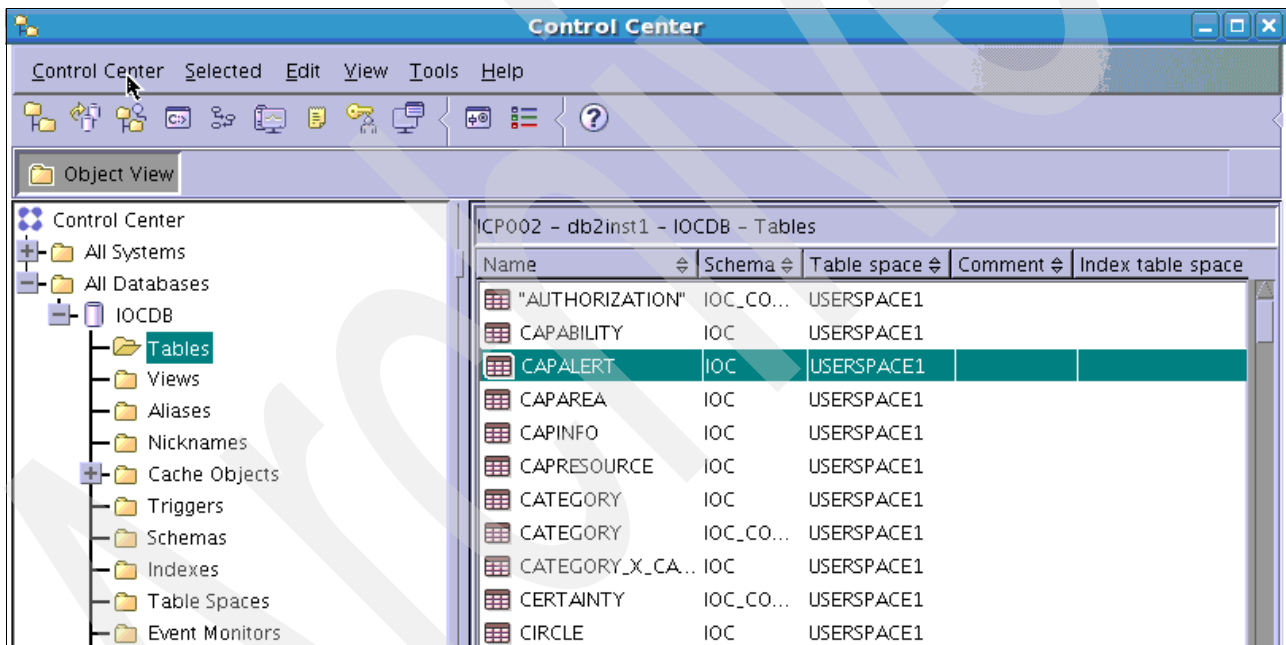


Figure 6-5 Database control center for IOCDB database

d. Verify that the event content matches the incoming data (Figure 6-6).

CAPAREAID	AREADESC	ALTITUDE	CEILING	GEOMETRY	CAPINFOID
afa478f3-2adc-...				COM.ibm.db2.jd...	56c5bcdf-1113-...
3c8d43be-bbae-...	West of I-75 clos...			COM.ibm.db2.jd...	cf4042fd-1c2a-...
2eaa9fa5-c00e-...	West of I-75 clos...			COM.ibm.db2.jd...	03c9714a-ce05-...
bd0ca211-851d-...	West of I-75 clos...			COM.ibm.db2.jd...	047005d7-0b3e-...
beb7c79b-1c57-...	West of I-75 clos...			COM.ibm.db2.jd...	0618d64d-5e92-...
17a53bb7-ffed-...	West of I-75 clos...			COM.ibm.db2.jd...	6de42551-79d5-...
1de6df8a-2450-...	West of I-75 clos...			COM.ibm.db2.jd...	795b1f6f-33f3-...
9ad0b917-d54f-...	Probe down 			COM.ibm.db2.jd...	b4ca2a13-24d3-...
51b8df10-1b2f-...	testing probe do...			COM.ibm.db2.jd...	6be6d68e-58be-...
469a9779-3b43-...	Flight to Miami De...			COM.ibm.db2.jd...	2e90c0e5-ec6c-...
100f6be0-5fbc-...	Probe down 			COM.ibm.db2.jd...	c3207fe3-b001-...

Figure 6-6 CAPALERT table - events list

Event server

To diagnose event issues on the event server, complete the following steps:

1. Check the following log files for any errors:
 - /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - /opt/IBM/netcool/omnibus/log/NCOMS.log
 - /opt/IBM/netcool/omnibus/log/NCO_PA.log
 - /opt/IBM/netcool/impact/log/NCI_policylogger.log

Logging: The `ioc_xml.log` file records the time stamp that the message is received from the external system and the CAP format of the message with its event identifier. The `NCOMS.log` file records the duplicate events. If the probe is down, the errors are logged in the `NCO_PA.log` file and the messages are also held in the queue (see Figure 6-11 on page 148). The `NCI_policylogger.log` file displays the actual logged values as processed by the policy if the debug flag is on.

Example 6-3 shows the `ioc_xml.log` file when events cannot be published to the queue because of a message bus service failure.

Example 6-3 Message bus failure highlighted in the `ioc_xml.log` file

```
2012-07-23T14:45:01: Debug: D-UNK-000-000: TransportType->      JMS
2012-07-23T14:45:01: Debug: D-UNK-000-000: TransportFile->
/opt/IBM/netcool/omnibus/java/conf/jmsTransport.properties
2012-07-23T14:45:01: Debug: D-JPR-000-000: Looking for transport type: JMS
2012-07-23T14:45:01: Debug: D-JPR-000-000: Looking for transport module class:
com.ibm.tivoli.netcool.integrations.transportmodule.JMSTransport
2012-07-23T14:45:01: Debug: D-JPR-000-000: Found transport class - instantiating
```

```

2012-07-23T14:45:01: Debug: D-JPR-000-000: Setting properties on class
com.ibm.tivoli.netcool.integrations.transportmodule.JMSTransport
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : queueName = 'jms/ioc.cap.out.q'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : queueConnectionFactory =
'jms/ioc.mb.con.factory'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : password = 'xxxxxx'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : providerURL =
'iiop://icp004.itso.ibm.com:10035'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : initialContextFactory =
'com.ibm.websphere.naming.WsnInitialContextFactory'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : queueName =
'jms/ioc.resource.out.q'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : username = 'mqm'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Transport property : queueName =
'jms/ioc.notification.out.q'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Creating initial context class using
'com.ibm.websphere.naming.WsnInitialContextFactory' and 'iiop://icp004.itso.ibm.com:1003
5'
2012-07-23T14:45:01: Debug: D-JPR-000-000: Looking up 'jms/ioc.mb.con.factory' in JNDI
2012-07-23T14:45:03: Debug: D-JPR-000-000: Creating queue connection using username 'mqm' and
password 'xxxxxxx'
2012-07-23T14:45:03: Information: I-UNK-000-000: Probewatch: Unable to get events; Caused by:
Failed to create JMS connection: JMSWMQ0018: Failed to connect to queue manager 'IOC.MB.QM' with
connection mode 'Client' and host name 'icp003.itso.ibm.com(1414)'
2012-07-23T14:45:03: Debug: D-UNK-000-000: Rules file processing took 32 usec.
2012-07-23T14:45:03: Debug: D-UNK-000-000: Flushing events to object servers
2012-07-23T14:45:03: Debug: D-UNK-000-000: Flushing events to object servers
2012-07-23T14:45:03: Error: E-JPR-000-000: Unable to get events
Caused by: Failed to create JMS connection: JMSWMQ0018: Failed to connect to queue manager
'IOC.MB.QM'

```

2. Ensure that the Intelligent Operations Center XML probe is running. Run the following **IOCControl** command from the management server to verify the status of the probe:

```
IOCControl status iocxml <password>
```

If the probe is off, use the following **IOCControl** command to start the IBM Tivoli Netcool/OMNIBus instance that automatically starts the probe:

```
IOCControl start ncob <password>
```

If the IBM Tivoli Netcool/OMNIBus is in running status, stop it by running the following **IOCControl** command:

```
IOCControl stop ncob <password>
```
3. Ensure that the service status of the EventProcessor, IOC_CAP_Event_Reader, and PolicyLogger is green. Use Event Processing and Enhancing, which is a web-based console for Tivoli Netcool/Impact, to verify the status.

For information about how to open the IBM Intelligent Operations Center web-based administration console, see 3.3, “Administration Consoles” on page 55. For an example of the expected service status, see Figure 6-7.

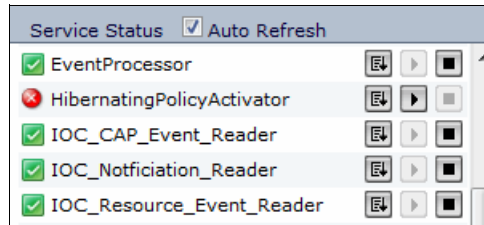


Figure 6-7 Event services in Service Status box

4. Verify that the event complies with the IOC_Update_CAPDB policy. Select **IOC** from the Policies drop-down menu. Figure 6-8 shows a snapshot of the event policy (IOC_Update_CAPDB).

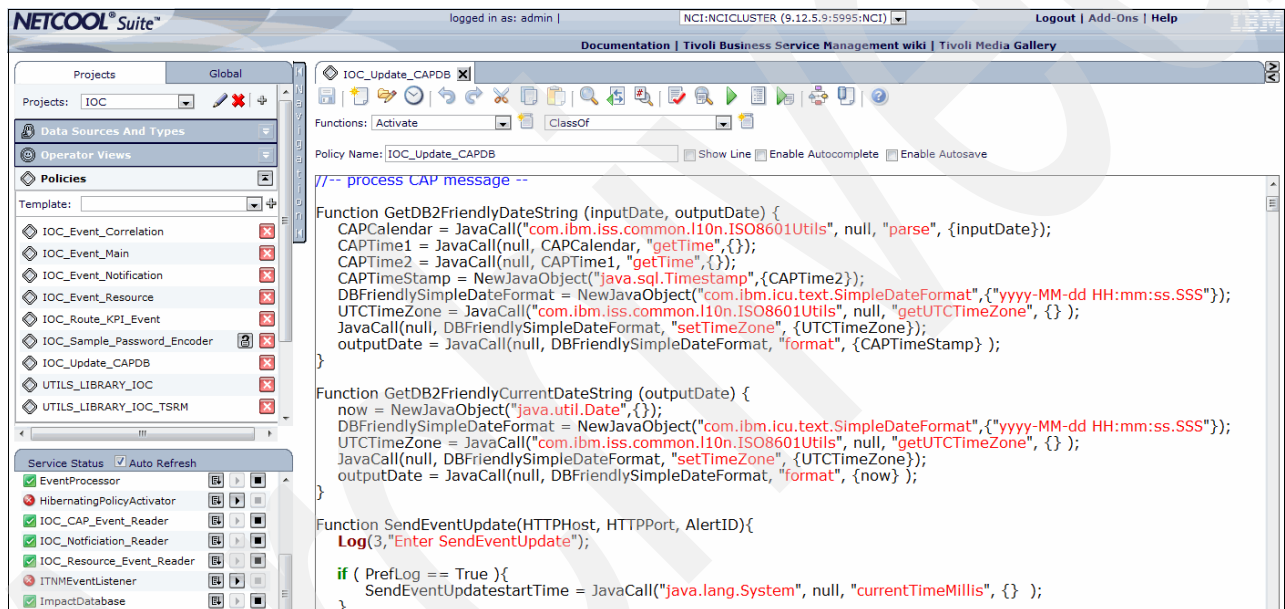


Figure 6-8 IOC_Update_CABDB policy on event processing and enhancing system

5. Verify that there are no duplicate events. The duplication occurs when the event with an existing event identifier comes into the system. Check the NCOMS.log file for duplication. Example 6-4 provides a sample error log when the event is duplicated.

Example 6-4 Duplication event sample error log

```

2012-07-18T09:41:18: Error: E-STK-102-013: [nstk]: NCOMS: Failed to register server's PID.
(-100:pid file exists, service already running)
2012-07-18T13:35:03: Error: E-AUT-002-006: Trigger "deduplicate_cap_alerts": action execution
failed: Attempt to insert duplicate row
2012-07-20T17:14:40: Error: E-AUT-002-006: Trigger "deduplicate_cap_alerts": action execution
failed: Attempt to insert duplicate row
2012-07-23T16:02:40: Error: E-OBX-102-023: Failed to authenticate user root. (-3600:Denied)
2012-07-23T16:02:40: Error: E-OBX-102-057: User root@icp003 failed to login: Denied
2012-07-24T13:11:01: Error: E-IVM-005-001: OpenServer - Error: 16113/10/0: Invalid object id
found in srv_putmsgg
  
```


2012-07-24T13:11:01: Error: E-IVM-005-001: OpenServer - Error: 16113/10/0: Invalid object id found in srv_putmsgq
 2012-07-24T13:11:01: Error: E-AUT-002-006: Trigger "deduplicate_cap_alerts": action execution failed: Attempt to insert duplicate row

- Verify that the event is not in the NCOMS database. To check this condition, open the NCOMS database console, as described in 3.8, “IBM Tivoli Netcool/OMNIBus database utility” on page 76, and check the alerts cap.infotable for the event.

Events are deleted from the NCOMS database after they are processed by the IOC_Update_CAPDB policy. If the events are in the NCOMS alerts.status table, that is an indication of an unsuccessful policy process or database server connection issue.

Figure 6-9 shows how the NCOMS alerts cap_info table gets populated when the IOC_CAP_Event_Reader or EventProcessor policy is stopped or the IOCDB database instance db2inst1 is stopped.

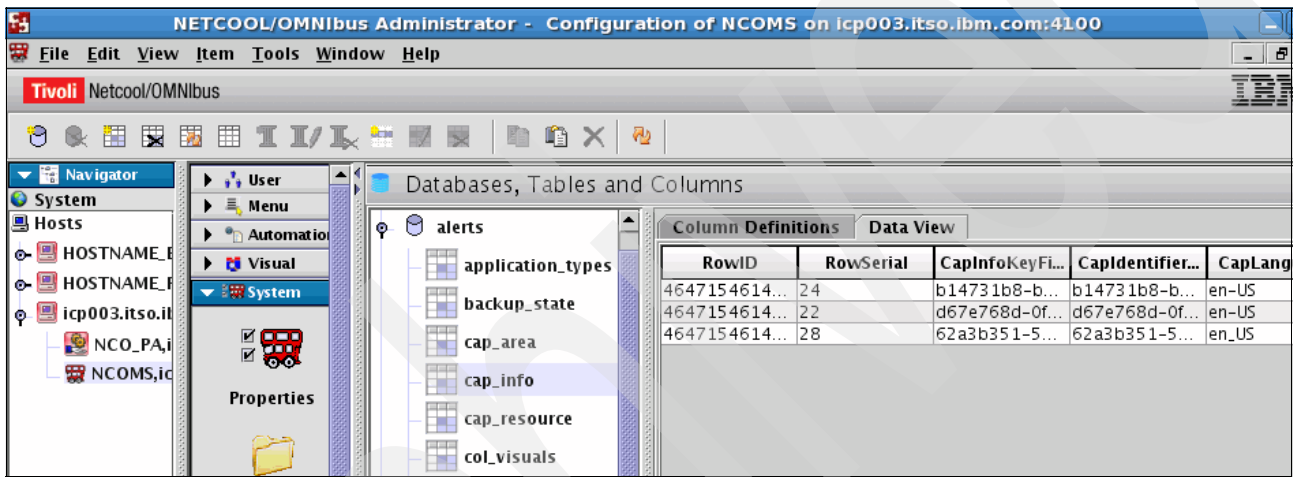


Figure 6-9 NCOMS or object server cap.info table accumulated data

- Check that the message bus is running. Use WebSphere MQ Explorer to verify the status. For information about starting and using WebSphere MQ Explorer, see 3.6, “WebSphere MQ Explorer” on page 72. Figure 6-10 shows when the queue manager is not running. In this situation, right-click and start the queue manager IOC.MB.QM.

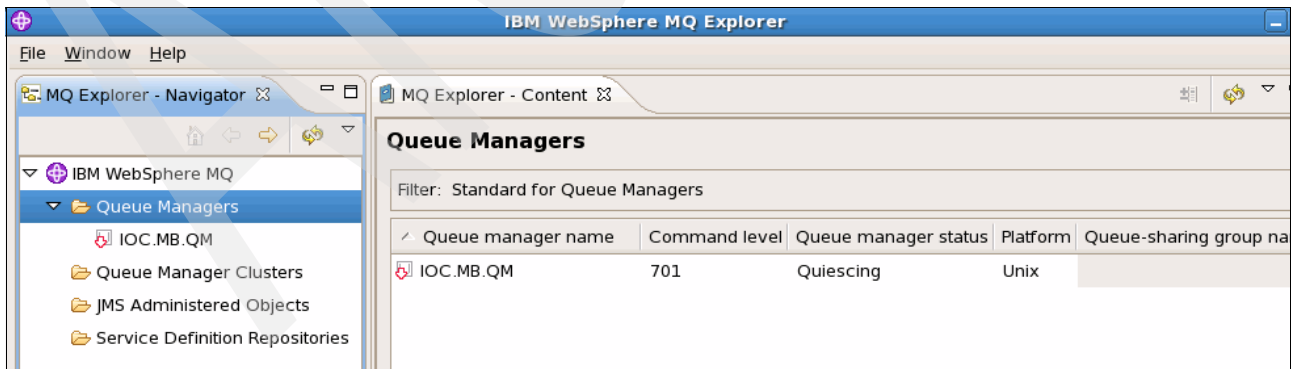


Figure 6-10 IOC.MB.QM queue manager is stopped

- Verify that the message queues IOC.CAP.IN and IOC_CAP_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY have a value of 0 in the Current Queue Depth field.

If the IOC.CAP.IN current queue depth is high, that is an indication that the message bus is not running. Figure 6-11 shows the Current Queue Depth field of IOC.CAP.IN as high.

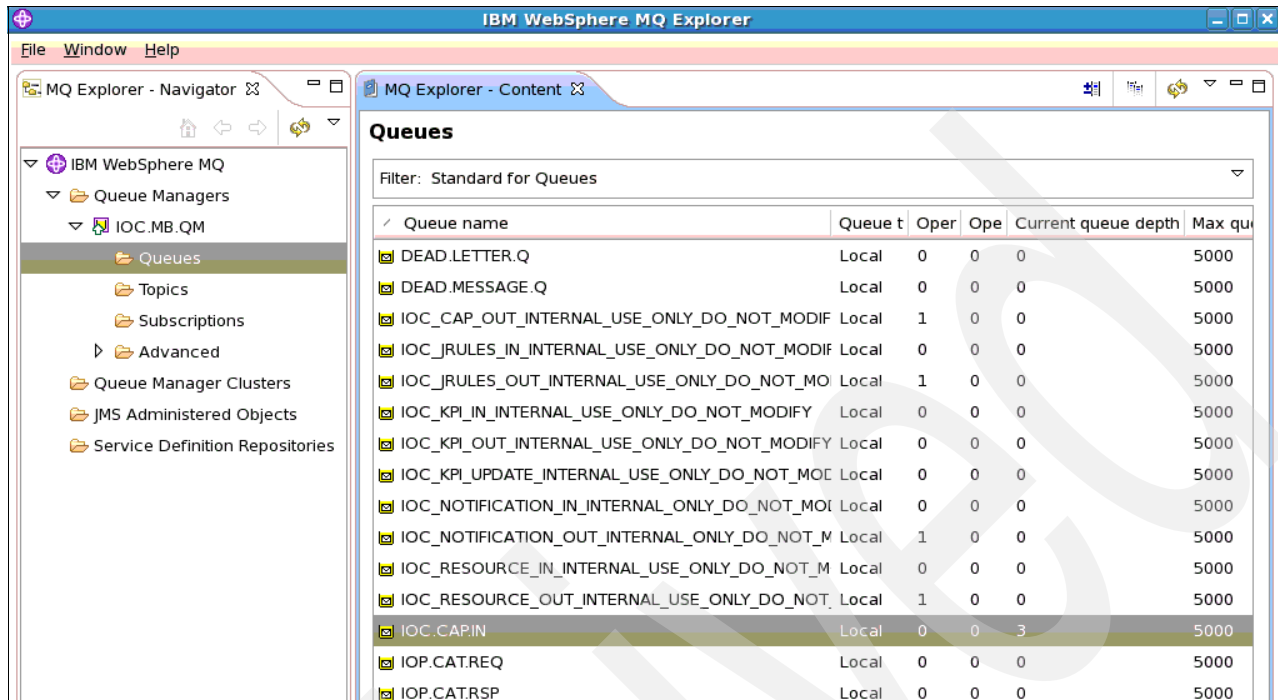


Figure 6-11 IBM WebSphere Message Broker is not running and IOC.CAP.IN queue depth is increasing

9. To restart the WebSphere Message Broker, run the following **IOControl** command:

```
./IOControl.sh start wmb <password>
```

Alternatively, the message bus can be started by completing the following steps:

a. Run the following commands:

```
xhost +
su - mqm
source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile
mqsilist
```

Here is the output of the broker name:

```
BIP1285I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is stopped.
BIP8071I: Successful command completion.
```

b. Restart WebSphere Message Broker by running the following command:

```
mqsisstart IOC_BROKER
```

Figure 6-12 shows when the probe is not running and the messages accumulate in the IOC_CAP_OUT queue (also called IOC_CAP_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY).

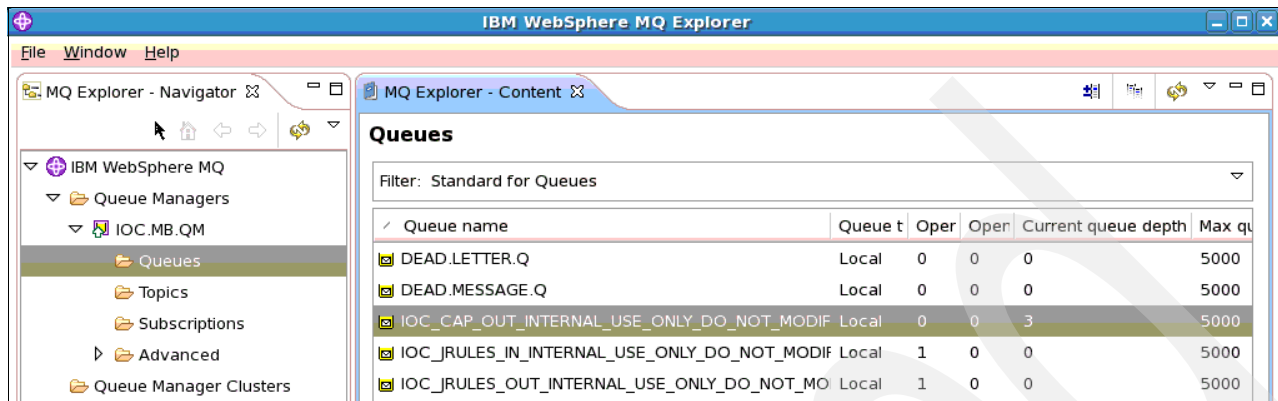


Figure 6-12 IOC_CAP_OUT message depth is 3

External event server

To diagnose event issues on the external event server, complete the following steps:

1. Verify that the communication between the IBM Intelligent Operations Center and the external server is working by running `ping`, which verifies if it is active.
2. Communicate with a third party to verify that the message is successfully sent from the external source.
3. If the IBM Intelligent Operations Center message bus is not working, the external source receives an error on their system. Figure 6-13 shows an error message when the message bus queue manager is not working.

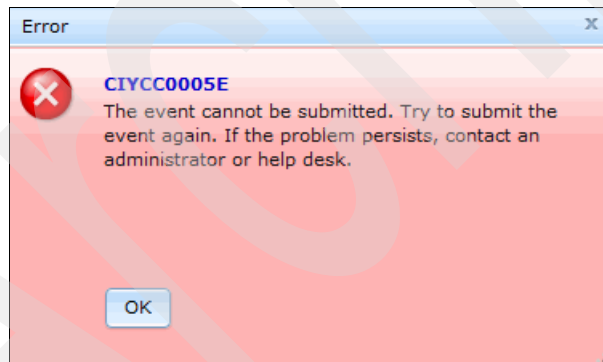


Figure 6-13 Event cannot be submitted when the message bus is stopped

6.1.2 Activities not displayed in the My Activities portlet

The My Activities portlet in IBM Intelligent Operations Center consists of assigned work that is associated with a standard operating procedure (SOP) where an authorized user is required to act according to the procedure.

Figure 6-14 shows how activities are displayed in the IBM Intelligent Operations Center MyActivities portlet.



Figure 6-14 My Activities portlet with assigned activities

This section provides a checklist of steps that you can perform to troubleshoot the scenario where work is triggered from an SOP workflow and it does not display in the assigned user's My Activity portlet.

Before you perform the troubleshooting steps in this section, gather the following information:

- ▶ A user ID that should receive the activities.
- ▶ An activity ID or name, if available.
- ▶ The SOP name that processes the work item.
- ▶ The workflow process that should trigger the activity.
- ▶ The event details, such as values for the Category, Severity, Urgency, and Certainty fields.

Application server

On the application server, complete the following steps:

1. Verify that all the services are running by using the System Verification Check tool. For information about running System Verification Check tests, see 3.2, "System Verification Check" on page 48.
2. Verify that the user is authorized to access the My Activities portlet. For details, see step 2 on page 140.
3. Ensure that the following portlet services are running. For details, see step 3 on page 141.
 - ioc_portal.ear
 - iss_curi.ear
 - iss_help.ear
 - iss_portal.ear
4. Verify that the portlet is visible on the Supervisor:Operations or Operator:Operations portal page.
5. Verify if the user is receiving other activities in the My Activities portlet.
6. Verify that there are no errors for the SOP in the following portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Event server

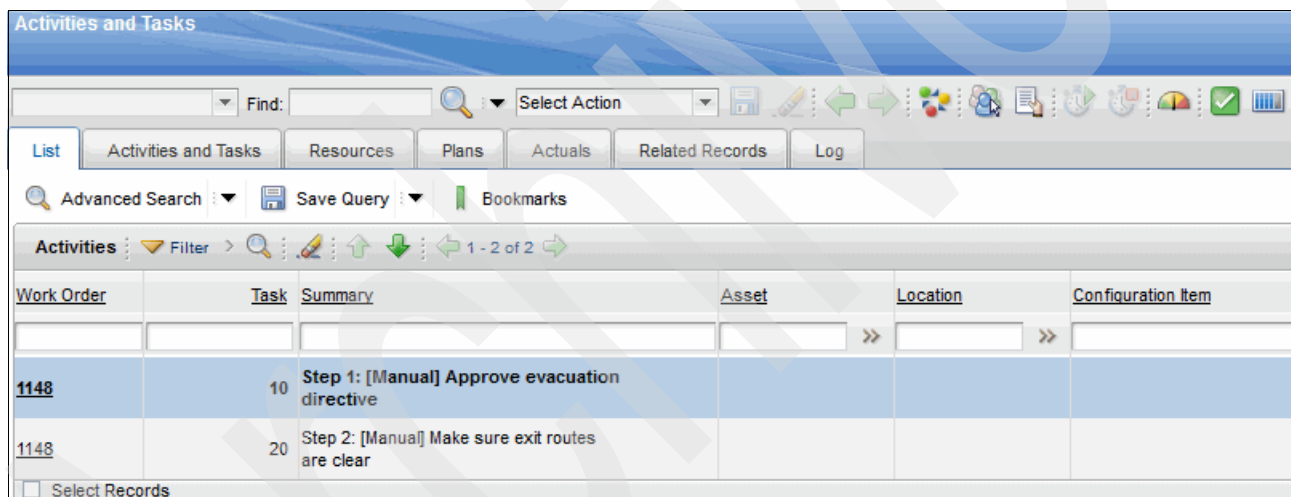
This section describes the verifications to perform on the event server.

Verify that the activity is displayed in the IBM Tivoli Service Request Manager on the Activities and Tasks page. Use the Standard Operating Procedure Administration (web-based console for Tivoli Service Request Manager Start Center) console to access the Activity and Tasks page. For information about starting the IBM Intelligent Operations Center web-based administration consoles, see 3.3, “Administration Consoles” on page 55.

Complete the following steps:

1. Log in to the IBM Intelligent Operations Center and click **Administration** → **Intelligent Operations** → **Administration Tools** → **Administration Consoles** → **Standard Operating Procedure Administration**.
2. Enter the administrator ID (maxadmin) and password.
3. From the main menu, click **Go To** → **Service Desk** → **Activities and Tasks**.
4. Press **Enter** on the Work Order field to list all the activities.

Figure 6-15 shows the activities of an SOP matching the event parameters with its associated SOP matrix.



Work Order	Task	Summary	Asset	Location	Configuration Item
1148	10	Step 1: [Manual] Approve evacuation directive			
1148	20	Step 2: [Manual] Make sure exit routes are clear			

Figure 6-15 SOP activities that are triggered by matching SOP matrix event

Activity is listed in IBM Tivoli Service Request Manager

If the activity is listed in the IBM Tivoli Service Request Manager Activities and Tasks page, but it is not displayed in the My Activities portlet, then it is a situation where the portal application is not synchronized with the IBM Tivoli Service Request Manager application. To recover from this condition and resolve this issue, restart the portal server by running the following **IOCCControl** commands on the management server:

```
cd /opt/IBM/ISP/mgmt/scripts
./IOCCControl.sh stop wpe <password>
./IOCCControl.sh start wpe <password>
```

Activity is not listed in IBM Tivoli Service Request Manager

If the activity is not listed in the IBM Tivoli Service Request Manager Activities and Tasks page, complete the following steps:

1. Verify that there are no errors in the `ioc_xml.log` policy log file by running the following command:

```
/opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Example 6-5 shows the error example. The 401 unauthorized HTTP error occurs when the IBM Tivoli Service Request Manager password is not set correctly in the event processing and enhancing service.

Example 6-5 Unauthorized access error in ioc_xml.log

```
26 Jul 2012 12:44:17,565: [IOC_Update_CAPDB] [MessageProcessor-Dog#7] Parser log:
TSRMPort before calling GetTSRMServerInfo:31015
26 Jul 2012 12:44:17,565: [IOC_Update_CAPDB] [MessageProcessor-Dog#7] Parser log:
MaxURL:http://icp003.itso.ibm.com:31015/meaweb/es/PLUSIOCEXTSYS/PLUSICrSOP
26 Jul 2012 12:44:17,593: [IOC_Update_CAPDB] [MessageProcessor-Dog#7] Parser log:
Error occurred in CAP db policy: Exception in policy: IOC_Update_CAPDB at line:
38.HTTP connection reported an error: 401 Unauthorized
26 Jul 2012 12:44:17,594: [IOC_Update_CAPDB] [MessageProcessor-Dog#7] Parser log:
ReturnCode:NULL
26 Jul 2012 12:44:17,594: [IOC_Update_CAPDB] [MessageProcessor-Dog#7] Parser log:
WORKORDERID:
```

To recover from this error, see the “Encrypting the Tivoli Service Request Manager administrative password” topic in the IBM Intelligent Operations Center Information Center at:

http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/install_encryptmaxpwd.html

2. Verify that the associated SOP is in the active status by completing the following steps:
 - a. Log in to IBM Tivoli Service Request Manager console, as described in 3.3, “Administration Consoles” on page 55.
 - b. From the main menu, click **Go To** → **Service Desk** → **Standard Operating Procedure**.
 - c. List the name of the SOP and check if the Status field is Active.
3. Verify that the SOP owner field is associated with a user group or user name by completing the following steps:
 - a. From the main menu, click **Go To** → **Service Desk** → **Standard Operating Procedure**.
 - b. Open the required SOP and verify that the Owner or Owner Group field is populated.

Figure 6-16 shows the SOP with its associated owners.

Sequence	Task	Instruction	Workflow Name	Owner	Owner Group
10	10	Step 1: [Manual] Approve evacuation directive			PLUSICTM
20	20	Step 2: [Manual] Make sure exit routes are clear			PLUSICTM

Figure 6-16 SOP with the steps and owners assigned

- c. Click the populated **Owner** → >> → **Go To People** and verify that Person exists and is in the Active status. You can click **Return** from the top menu to return to the SOP page.
- d. Click the populated **Owner Group** → >> → **Go To Person Groups** and verify that Person Group exists and is in the Active status.

Figure 6-17 shows the SOP associated with Person Groups and its associated persons.

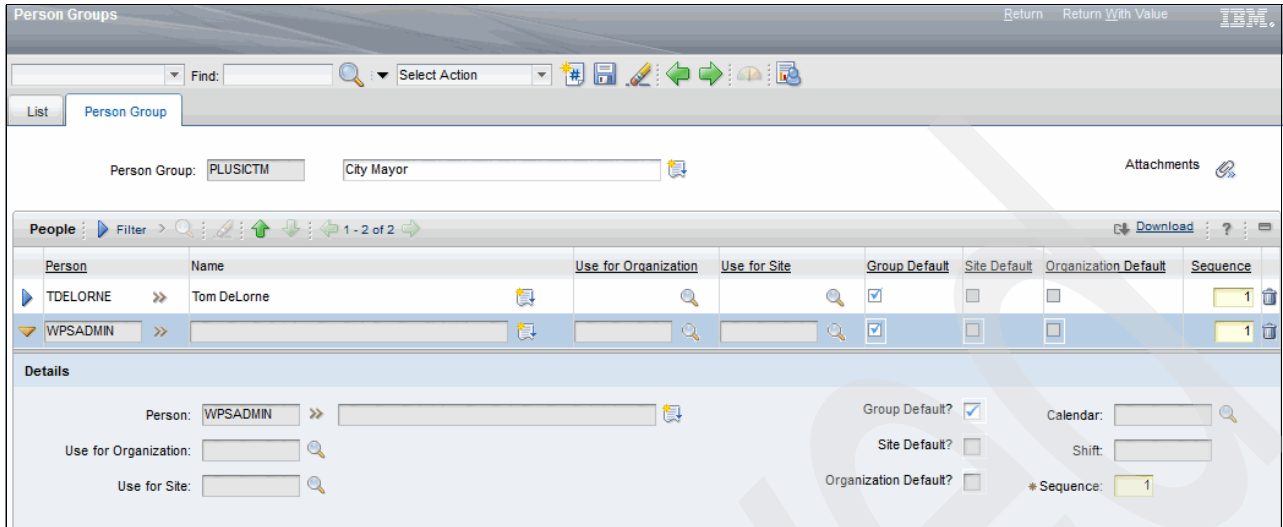


Figure 6-17 WPSADMIN Person group that is associated with wpsadmin

- e. Click **Person Details** → **Go To People** and verify that the person exists and is in the Active status (Figure 6-18).

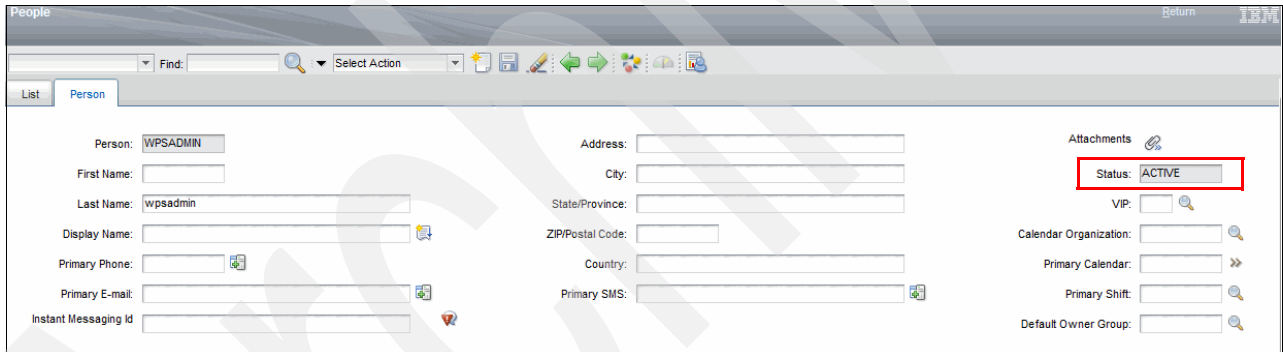


Figure 6-18 Person is in the Active status

4. Verify that the SOP is associated with an SOP selection matrix by completing the following steps:
 - a. From the main menu, click **Go To** → **Service Desk** → **SOP Selection Matrix**.
 - b. Verify that the SOP Name field in the SOP Selection Matrix is part of at least one matrix row.

- Verify that the incoming event values match the SOP Selection Matrix with its Category, Severity, Urgency, and Certainty fields. Figure 6-19 shows the event parameters in the SOP Matrix that is mapped to a specific SOP.

Category	Severity	Urgency	Certainty	SoP Name
Met	Severe	Future	Observed	PLUSIMITIG
Met	Severe	Future	Likely	PLUSIMITIG
Met	Extreme	Future	Observed	PLUSIPREPA
Met	Extreme	Future	Likely	PLUSIPREPA
Met	Extreme	Immediate	Observed	PLUSIRESPO

Figure 6-19 SOP associated with a SOP Matrix

6.1.3 KPIs not displayed in the Status or Drill Down portlets

KPI flow: The troubleshooting process that is described in this section is driven by the IBM Intelligent Operations Center KPI flow. For information about the KPI flow, see 7.2, “Key performance indicators flow” on page 196.

This section describes the step by step process to troubleshoot the Key Performance Indicators (KPIs) not displayed on portal issue.

Message flows: Because the KPI message flow and events message flows are similar, most of the steps that are covered in this section are already described in 6.1.1, “Events that are not displayed in the Details portlet” on page 138. Reading 6.1.1, “Events that are not displayed in the Details portlet” on page 138 is a prerequisite for understanding the information that is presented in this section.

It is important to understand a basic KPI message. Example 6-6 shows a sample KPI event in CAP format that is published to the IBM Intelligent Operations Center server.

Example 6-6 KPI sample message

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
  <cap:identifier>Msg25:WaterQualityOne</cap:identifier>
  <cap:sender>Water</cap:sender>
  <cap:sent>2012-07-26T12:48:00-05:00</cap:sent>
  <cap:status>Actual</cap:status>
  <cap:msgType>Alert</cap:msgType>
  <cap:scope>Public</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
    <cap:category>Env</cap:category>
```

```
<cap:event>Water_Quality</cap:event>
<cap:urgency>Immediate</cap:urgency>
<cap:severity>Severe</cap:severity>
<cap:certainty>Observed</cap:certainty>
<cap:headline>Water Quality</cap:headline>
<cap:description>Water Quality</cap:description>
<cap:onset>2012-07-26T11:48:00-05:00</cap:onset>
<cap:senderName>Water</cap:senderName>
<cap:parameter>
  <cap:va lueName>PH</cap:va lueName>
  <cap:va lue>Acceptable</cap:va lue>
</cap:parameter>
<cap:parameter>
  <cap:va lueName>Turbidity</cap:va lueName>
  <cap:va lue>acceptable</cap:va lue>
</cap:parameter>
</cap:info>
</cap:alert>
```

Notice the following items:

- ▶ The code element is set to KPI.
- ▶ The onset element represents the time and date the subject of the event is expected to occur and is used for most KPI calculations. For information about creating sample KPI messages with the IBM Intelligent Operations Center Event Publisher tool, see 3.4.2, “Creating test KPI messages” on page 62.

Use the following sections to diagnose KPI issues by logging in to the different servers with administration credentials and performing the steps that are described for each server.

Application server

On the application server, complete the following steps:

1. Verify that all the services are running by using the System Verification Check tool. For more information about running System Verification Check tests, see 3.2, “System Verification Check” on page 48.

Important: It is important to confirm that Tivoli Monitoring Enterprise Monitoring server and IBM Tivoli Monitoring Enterprise Portal server are running. Run the following **IOControl** commands to verify the status of these servers:

- ▶ **IOControl.sh status tems <password>**
- ▶ **IOControl.sh status teps <password>**

2. Verify that the user is authorized to access the portal page and the portlet. For information about users’ access to portal resources, see 5.2.2, “Portal resource permissions and user role groups” on page 111.

3. Verify that the Status or Key Performance Indicator Drill Down portlets are visible on the Supervisor:Status portal page. Figure 6-20 shows the page when the portlets are visible.

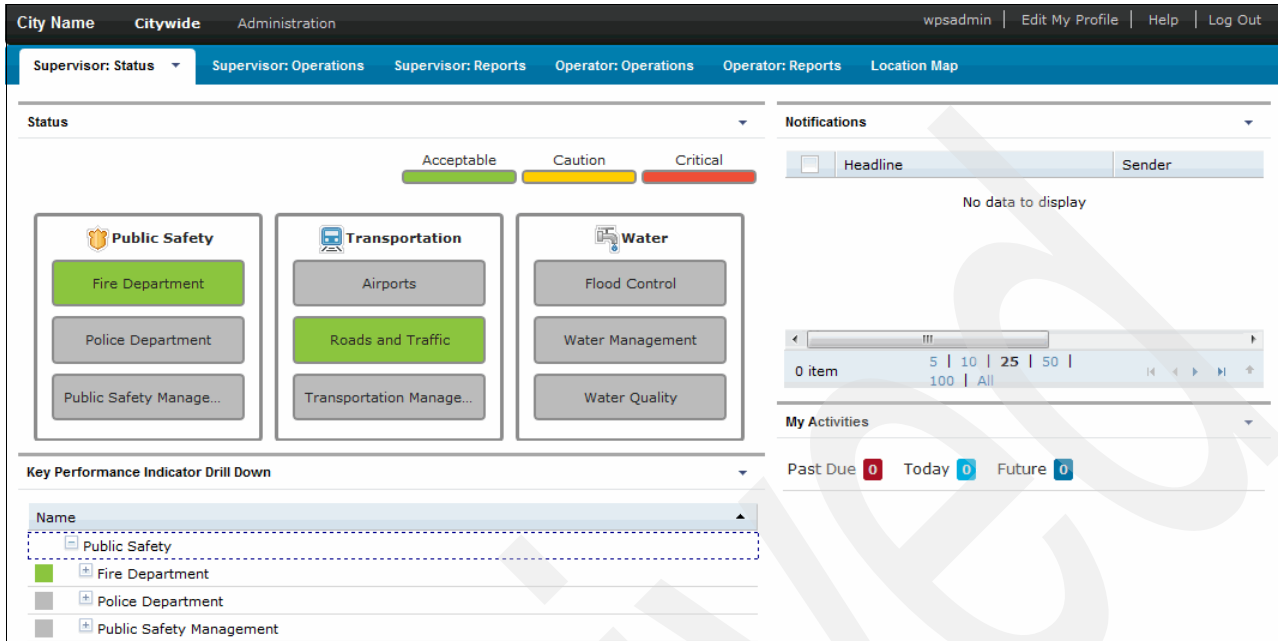


Figure 6-20 KPI portlets on the Supervisor: Status page

4. Check whether the Status portlet is displaying other KPIs.
5. Verify that there are no failed services in the application server by completing the following steps:
 - a. Log in to the Application Server web-based console. For information about starting a web-based console, see 3.3, “Administration Consoles” on page 55.

- b. Click **Troubleshooting** → **Monitor Models** → **Failed Event Sequences** (Figure 6-21).

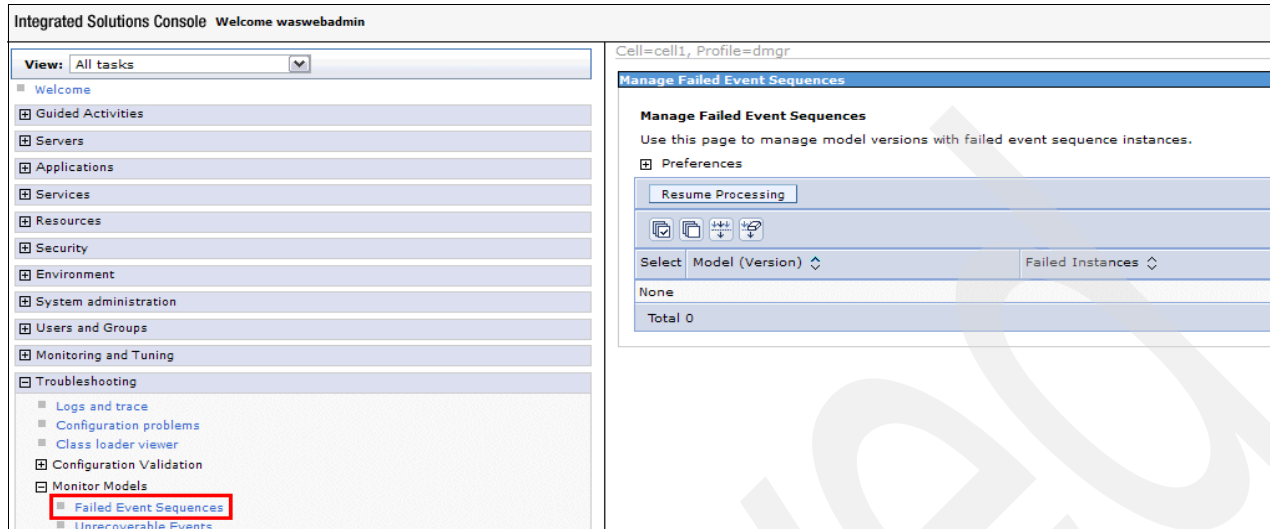


Figure 6-21 Failed event sequences

- c. If KPI events are listed, delete them and restart the business monitoring server. From the Application Server console, click **Applications** → **Monitor Services** → **Recorded Events Management** → **Events Management**.
- d. Confirm that for every KPI event that is sent, at least two events are created on the Events Management view. This creation verifies that events reached the business monitoring service (Figure 6-22).

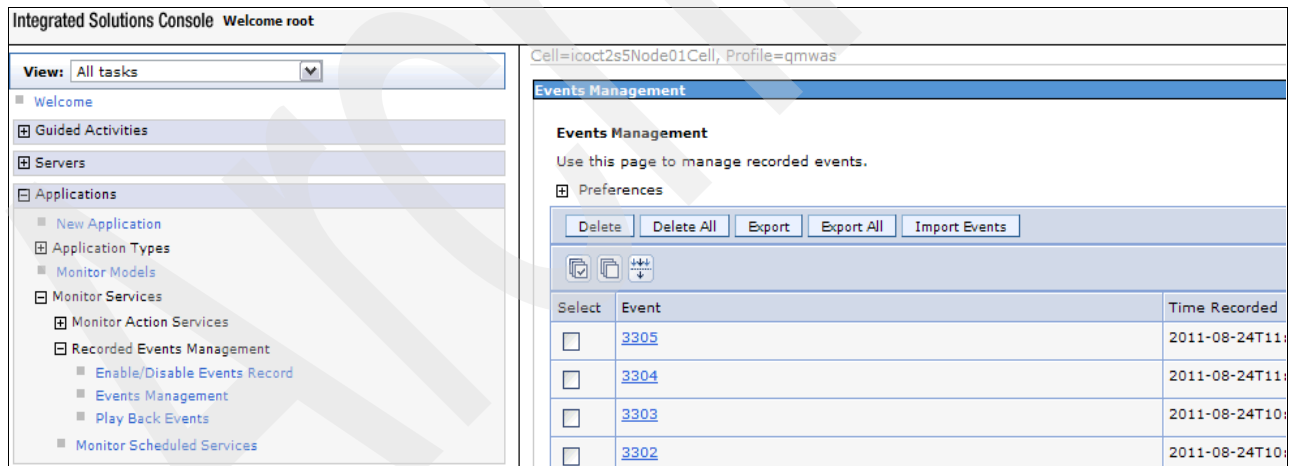


Figure 6-22 Events Management display

6. Verify that the following portlet services are running. For details, see step 3 on page 141.
- ioc_portal.ear
 - iss-curi.ear
 - iss_help.ear
 - iss-portal.ear

7. Verify that there are no errors in the following monitor logs:
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/nodeagent/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/nodeagent/SystemErr.log
8. Verify that there are no errors in the following portal logs for the KPI:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Database server

Events are stored in the IOC.CAPALERT table under the db2inst1 instance. To check the contents of this table, complete the following steps on the database server:

1. Log in to the database server.
2. Run the following commands:


```
su - db2inst1
db2cc &
```
3. Figure 6-23 shows a snapshot of KPI messages in the CAPALERT table.

CAPALERTID	IDENTIFIER	SENDER	SENT	STATUS	MSGTYPE
b6263686-5dd5...	31dc0b5f-27c4-...	Police	Jul 24, 2012 8:4...	Actual	Alert
45703d14-7308...	8e7eb7a8-e259...	wpsadmin	Jul 24, 2012 4:0...	Actual	Alert
aa5732d8-0900...	43698d85-2f14...	Police	Jul 24, 2012 8:4...	Actual	Alert

Figure 6-23 KPI messages in the CAPALERT table

Event server

On the event server, complete the following steps:

1. Verify that the queue manager, IOC.MB.QM, is running by checking it in WebSphere MQ Explorer. For information about starting WebSphere MQ Explorer, see 3.6, “WebSphere MQ Explorer” on page 72.

2. Ensure that the following queues have a value of 0 in the Current Queue Depth field:
 - IOC_KPI_IN (also called IOC_KPI_IN_INTERNAL_USE_DO_NOT_MODIFY)
 - IOC_KPI_OUT (also called IOC_KPI_OUT_INTERNAL_USE_DO_NOT_MODIFY)
 - IOC_KPI_UPDATE (also called IOC_KPI_UPDATE_INTERNAL_USE_DO_NOT_MODIFY)
 - IOC_CAP_IN
 - IOC_CAP_OUT

Messages that are held in the following queues are a symptom for one or more of the following problems:

- IOC.CAP.IN: The message queue is running while the WebSphere Message Broker is stopped.
- IOC_CAP_OUT: WebSphere Message Broker is running while the probe is stopped.
- IOC_KPI_IN: The policy is running while the WebSphere Message Broker is stopped during the processing of a KPI.
- IOC_KPI_OUT: WebSphere Message Broker is running while the monitor is stopped.
- IOC_KPI_UPDATE: The Message Driven Bean (MDB) to update the KPI status on the portlet is down.

Figure 6-24 shows that the message bus was down during the processing of KPI messages by the policy. Therefore, the messages are accumulated in the IOC_KPI_IN queue (also called IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY queue).

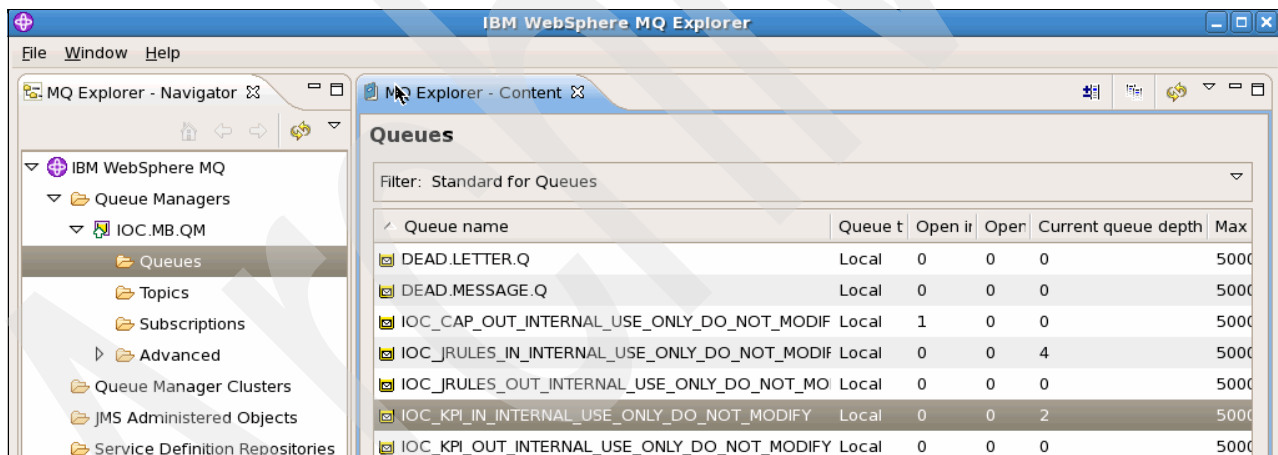


Figure 6-24 Message bus down and accumulating messages in the IOC_KPI_IN queue

3. Verify that the Open Input Count field is 0 for the queues that are listed in step 2. This value indicates that the connected service failed. If any of the queues has the Open Input Count field set to 0, complete the following steps on the application server:
 - a. Open the Application Server web-based administration console.
 - b. Click **Servers** → **Clusters** → **WebSphere Application Server clusters**.

- c. Select the monitor application **WBM_DE.AppTarget** and click **Stop**. Figure 6-25 shows the status of the monitor application when it is stopped.

Stopped server: Wait until the server is stopped and is solid red. Click the **Refresh** icon next to the Status option to refresh the application status.

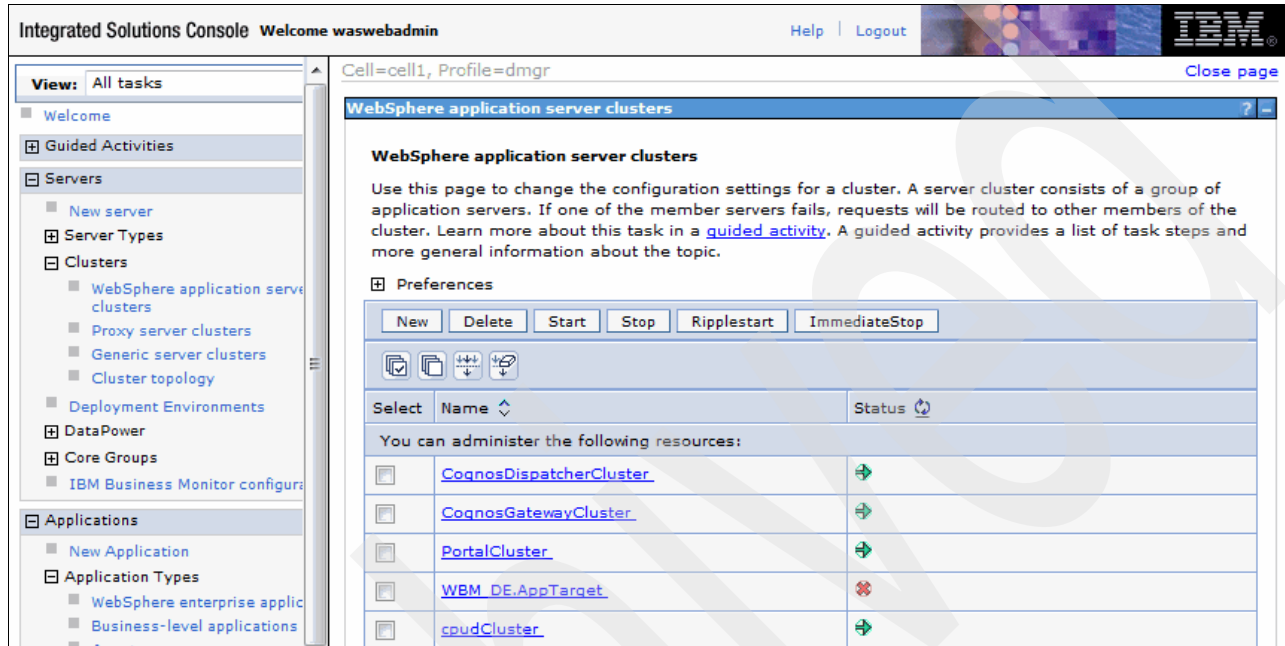


Figure 6-25 WebSphere Business Monitor application stopped

- d. Select the monitor application **WBM_DE.AppTarget** and click **Start**. This operation restarts the monitor cluster and message queue connection.
- e. Check the following log files for any errors:
 - /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - /opt/IBM/netcool/omnibus/log/NCOMS.log
 - /opt/IBM/netcool/omnibus/log/NCO_PA.log
 - /opt/IBM/netcool/impact/log/NCI_policylogger.log

Logs: The `ioc_xml.log` file records the time stamp when the message was received from the external system, and the CAP format of the message with its event identifier. The `NCOMS.log` file records the duplicate events. If the probe is down, the errors are logged in the `NCO_PA.log` file. The `NCI_policylogger.log` file displays the actual logged values as processed by the policy if the debug flag is on.

Example 6-7 shows a snapshot for the `ioc_xml.log` file for a processed KPI message. Notice the highlighted sections of a successful KPI transaction.

Example 6-7 KPI message in `ioc_xml.log`

```
2012-07-25T16:53:23: Debug: D-JPR-000-000: Adding message from endpoint
'jms/ioc.cap.out.q' to queue
2012-07-25T16:53:23: Debug: D-JPR-000-000: Received message from endpoint
jms/ioc.cap.out.q: <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```

<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>0aaebcca-eaf8-4b96-823d-cd482d125253</identifier>
  <sender>Water</sender>
  <sent>2012-02-17T15:47:00-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>KPI</code>
  <info>
    <category>Env</category>
    <event>Water_Quality</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <onset>2012-02-17T15:47:00-05:00</onset>
    <senderName>Water</senderName>
    <headline>Water Quality</headline>
    <description>Water Quality</description>
    <parameter>
      <valueName>PH</valueName>
      <value>Acceptable</value>
    </parameter>
    <parameter>
      <valueName>Turbidity</valueName>
      <value>acceptable</value>
    </parameter>
  </info>
</alert>

```

2012-07-25T16:53:23: Debug: D-JPR-000-000: **Looking for transformer for endpoint: jms/ioc.cap.out.q**

2012-07-25T16:53:23: Debug: D-JPR-000-000: **Parsing transformed message:**

identifier:string:"0aaebcca-eaf8-4b96-823d-cd482d125253"

sender:string:"Water"

sent:utc:"2012-02-17T15:47:00-05:00"

sentTime:string:"2012-02-17T15:47:00-05:00"

status:string:"Actual"

msgType:string:"Alert"

scope:string:"Public"

code_01:string:"KPI"

infos:integer:"1"

info_01_language:string:""

info_01_category:string:"Env"

info_01_event:string:"Water_Quality"

info_01_urgency:string:"Immediate"

info_01_severity:string:"Severe"

info_01_certainty:string:"Observed"

info_01_onset:utc:"2012-02-17T15:47:00-05:00"

info_01_onsetTime:string:"2012-02-17T15:47:00-05:00"

info_01_senderName:string:"Water"

info_01_headline:string:"Water Quality"

info_01_description:string:"Water Quality"

parameters:integer:"2"

info_01_parameter_01_Name:string:"PH"

info_01_parameter_01_Value:string:"Acceptable"


```

info_01_parameter_02_Name:string:"Turbidity"
info_01_parameter_02_Value:string:"acceptable"
resources:integer:"0"
areas:integer:"0"
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] TransformerName:
cap2nvpairs
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] Endpoint:
jms/ioc.cap.out.q
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] identifier:
0aaebcca-eaf8-4b96-823d-cd482d125253
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] sender: Water
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] sent: 1329511620
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] sentTime:
2012-02-17T15:47:00-05:00
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] status: Actual
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] msgType: Alert
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] scope: Public
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] code_01: KPI
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] infos: 1
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_language:
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_category:
Env
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_event:
Water_Quality
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_urgency:
Immediate
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_severity:
Severe
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_certainty:
Observed
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_onset:
1329511620
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_onsetTime:
2012-02-17T15:47:00-05:00
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_senderName:
Water
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_headline:
Water Quality
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] info_01_description:
Water Quality
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] parameters: 2
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor]
info_01_parameter_01_Name: PH
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor]
info_01_parameter_01_Value: Acceptable
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor]
info_01_parameter_02_Name: Turbidity
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor]
info_01_parameter_02_Value: acceptable
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] resources: 0
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] areas: 0
2012-07-25T16:53:23: Debug: D-UNK-000-000: [Event Processor] Processing alert {0
remaining}
2012-07-25T16:53:23: Debug: D-UNK-000-000: <<<< Entering... XML CAP Rules>>>>

```

- Verify that the probe is running by running the following **IOControl** command:

```
IOControl status iocxml <password>
```

If the probe is not running, run the following **IOControl** command to start IBM Tivoli Netcool/OMNIBus, which automatically starts the probe if it is down. If the IBM Tivoli Netcool/OMNIBus is running, stop it and then start it.

```
IOControl start ncoib <password>
```

Figure 6-26 shows the accumulation of KPIs in the NCOMS database when the probe is down.

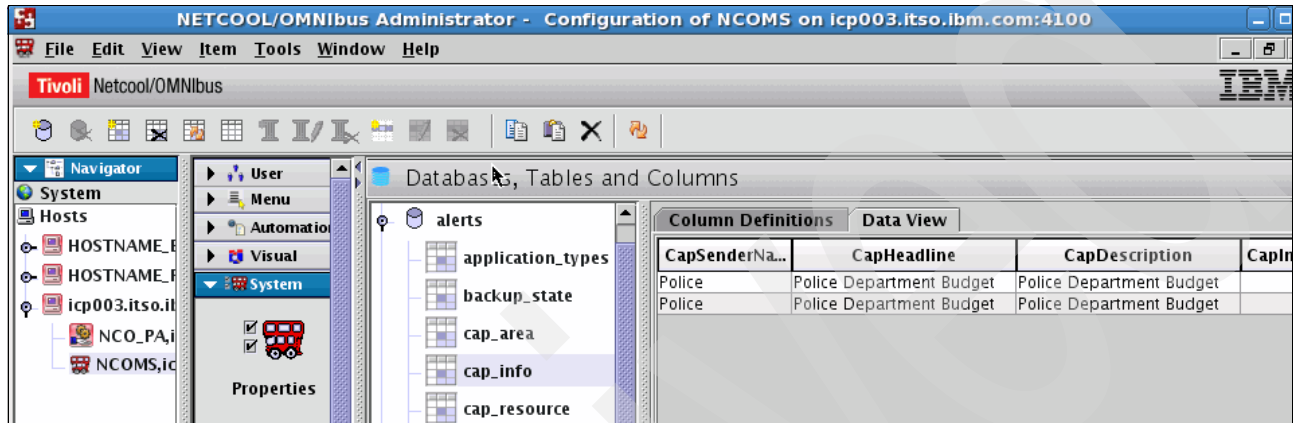


Figure 6-26 NCOMS accumulation of KPI messages

- Verify that the service status of the Event_Processor, IOC_CAP_Event_Reader, and PolicyLogger is green. For details about opening the Event Processing and Enhancing console, see 3.3, “Administration Consoles” on page 55.
- Verify that the event complies with the IOC_Route_KPI policy. The XML message must contain at least an element of name code with a value of KPI.

External event source

On the external event server, complete the following steps:

- Verify that the communication between the IBM Intelligent Operations Center and the external server is working by running **ping** to verify if the link is active.
- Communicate with a third party to verify that the message was successfully sent from the external source.
- If the IBM Intelligent Operations Center message bus is not working, the external source receives an error on their system. Figure 6-13 on page 149 shows an error message when the message bus queue manager is not working.

6.1.4 Notifications not displayed in portlet

Notification flow: The troubleshooting process that is described in this section is driven by the IBM Intelligent Operations Center notification flow. For information about the notification flow, see 7.4, “Notification flow” on page 206.

Notifications are plain XML that indicate a message is received or changed. It is received in IBM Intelligent Operations Center from two different sources:

- ▶ IOC internal: When a KPI changes color or crosses its threshold, the business monitoring system publishes notification messages.
- ▶ IOC external: When an external system sends a notification on previously received messages or correlated events from IBM Intelligent Operations Center.

These messages are then published in the Notification portlet in IBM Intelligent Operations Center Supervisor:Operations or Operator:Operations portal page.

Notifications: Most of the troubleshooting steps for notifications that are not displayed in the Notifications portlet are similar and already detailed in 6.1.1, “Events that are not displayed in the Details portlet” on page 138. Reading 6.1.1, “Events that are not displayed in the Details portlet” on page 138 is a prerequisite to understanding the information in this section.

Example 6-8 shows a KPI notification XML message when the color of the KPI status changes in the IBM Intelligent Operations Center. Notice that the notification ID and notificationType elements are populated.

Example 6-8 KPI notification XML message

```
<?xml version="1.0" encoding="UTF-8" ?>
<notification xmlns="urn:ibm:industry:solutions:ioc:notification:1.0">
<notificationId>f30a31c9-6d1f-48f5-80a8-998e3e22d9cf</notificationId>
<notificationType>Alert</notificationType>
<sentFrom>KPI System</sentFrom>
<sentToGroup>;CityWideExecutive;CityWideSupervisor;</sentToGroup>
<headline>{"KPI ID": "pH", "kpi.CHANGED": "kpi.CHANGED"}</headline>
<description>kpi.CHANGED</description>
<kpiLink>pH</kpiLink>
<category>Infra</category>
<parameter>
<parameterName>pH</parameterName>
</parameter>
</notification>
```

Use the following sections to diagnose notification issues by logging in to the different servers with administration credentials and completing the steps for each server.

Database server

Events are stored in the IOC.NOTIFICATION table under the db2inst1 instance. You can check this table by completing the following steps on the database server:

1. Log in to the database server and run the following commands:

```
su - db2inst1
db2cc &
```

2. The NOTIFICATION table contents are displayed (Figure 6-27).

NOTIFICATIONID	TYPE	CATEGORY	SENTTIMESTAMP	SENTFROM	SENTTOGROUP	SE
8a940977-23e9...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
50df50cf-1452-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
0a1cd410-6db1...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
855efc98-23d4-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
76af2720-9e73-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
873d2336-e733...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
7df20712-94dd...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
10447a57-9bf3...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
5c4137cd-e74a-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
759a0774-0e0d...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
6ddf653d-2e37...	Test		Jul 23, 2012 3:3...	CCT	wpsadmins	
22447fef-dfa0-4...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
73eefe55-50e0-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
8c934a89-1eb2...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	
fb2656c7-1968-...	Alert	Fire	Jul 18, 2012 5:3...	Correlation Engine	;CityWideExecutiv...	

Figure 6-27 Messages in the NOTIFICATION table

Event server

Complete the following steps on the event server:

1. Verify that the queue manager IOC.MB.QM is running by checking it with WebSphere MQ Explorer. For more information about starting and using WebSphere MQ Explorer, see 3.6, “WebSphere MQ Explorer” on page 72.
2. Check that the IOC_NOTIFICATION_IN and IOC_NOTIFICATION_OUT queues have a value of 0 in the Current Queue Depth field.
3. Check the following log files for errors:
 - /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - /opt/IBM/netcool/omnibus/log/NCOMS.log
 - /opt/IBM/netcool/omnibus/log/NCO_PA.log
 - /opt/IBM/netcool/impact/log/NCI_policylogger.log

Important: The `ioc_xml.log` file records the time stamp when the message was received from the external system, and the CAP format of the message with its event identifier. The `NCOMS.log` file records the duplicate events, if any. If the probe is down, the errors are logged in the `NCO_PA.log` file. The `NCI_policylogger.log` file displays the actual logged values as processed by the policy if the debug flag is on.

Example 6-9 shows a sample successful KPI notification message that is logged in `ioc_xml.log`. Notice the highlighted section for notification details, the rules that are applied, and the endpoint queue to which it is published.

Example 6-9 KPI Notification ioc_xml.log snapshot

```
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] Endpoint:
jms/ioc.notification.out.q
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] notificationId:
298d410f-bf85-4210-be3a-efc257bd3594
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] notificationType:
Alert
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] sentFrom: KPI
System
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] sentToGroup:
;CityWideExecutive;CityWideSupervisor;
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] headline: {"KPI
ID":"Physical_Indicators","kpi.CHANGED":"kpi.CHANGED"}
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] description:
kpi.CHANGED
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] kpiLink:
Physical_Indicators
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] category: Infra
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] parameters:
1
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor]
parameter_01_parameterName: Physical_Indicators
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor]
parameter_01_parameterValue:
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] Processing alert
{0 remaining}
2012-07-25T16:34:13: Debug: D-UNK-000-000: <<<<< Entering...
xml_notification.rules >>>>>
2012-07-25T16:34:13: Debug: D-UNK-000-000: Executing genevent() command for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() created new alert for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() created new alert for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() sent new event to target
server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: <<<<< Leaving...
xml_notification.rules >>>>>
2012-07-25T16:34:13: Debug: D-UNK-000-000: Rules file processing took 223 usec.
2012-07-25T16:34:13: Debug: D-UNK-000-000: Flushing events to object servers
2012-07-25T16:34:13: Debug: D-JPR-000-000: Adding message from endpoint
'jms/ioc.notification.out.q' to queue
2012-07-25T16:34:13: Debug: D-JPR-000-000: Received message from endpoint
jms/ioc.notification.out.q: <?xml version="1.0" encoding="UTF-8"?><notification
xmlns="urn:ibm:industry:solutions:ioc:notification:1.0"><notificationId>272b43a
4-4a4e-4336-95ac-7dc597114d51</notificationId><notificationType>Alert</notifica
tionType><sentFrom>KPI
System</sentFrom><sentToGroup>;CityWideExecutive;CityWideSupervisor;</sentToGro
up><headline>{"KPI
ID":"Water_Quality","kpi.CHANGED":"kpi.CHANGED"}</headline><description>kpi.CHA
```

```

NGED</description><kpiLink>Water_Quality</kpiLink><category>Infra</category><parameter><parameterName>Water_Quality</parameterName></parameter></notification>
2012-07-25T16:34:13: Debug: D-JPR-000-000: Looking for transformer for
endpoint: jms/ioc.notification.out.q
2012-07-25T16:34:13: Debug: D-JPR-000-000: Parsing transformed message:
notificationId:string:"272b43a4-4a4e-4336-95ac-7dc597114d51"
notificationType:string:"Alert"
sentFrom:string:"KPI System"
sentToGroup:string:";CityWideExecutive;CityWideSupervisor;"
headline:string:{"KPI ID":"Water_Quality","kpi.CHANGED":"kpi.CHANGED"}"
description:string:"kpi.CHANGED"
kpiLink:string:"Water_Quality"
category:string:"Infra"
parameters:integer:"1"
parameter_01_parameterName:string:"Water_Quality"
parameter_01_parameterValue:string:""
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] TransformerName:
notification2nvpairs
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] Endpoint:
jms/ioc.notification.out.q
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] notificationId:
272b43a4-4a4e-4336-95ac-7dc597114d51
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] notificationType:
Alert
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] sentFrom: KPI
System
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] sentToGroup:
;CityWideExecutive;CityWideSupervisor;
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] headline: {"KPI
ID":"Water_Quality","kpi.CHANGED":"kpi.CHANGED"}
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] description:
kpi.CHANGED
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] kpiLink:
Water_Quality
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] category: Infra
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] parameters:
1
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor]
parameter_01_parameterName: Water_Quality
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor]
parameter_01_parameterValue:
2012-07-25T16:34:13: Debug: D-UNK-000-000: [Event Processor] Processing alert
{0 remaining}
2012-07-25T16:34:13: Debug: D-UNK-000-000: <<<<< Entering...
xml_notification.rules >>>>>
2012-07-25T16:34:13: Debug: D-UNK-000-000: Executing genevent() command for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() created new alert for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() created new alert for
target server 'Notification'.
2012-07-25T16:34:13: Debug: D-UNK-000-000: genevent() sent new event to target
server 'Notification'.

```

```
2012-07-25T16:34:13: Debug: D-UNK-000-000: <<<<< Leaving...
xml_notification.rules >>>>>
```

4. Check that the probe is running. Run the following **IOControl** command on the management server:

```
IOControl status iocxml <password>
```

If the probe is not running, start IBM Tivoli Netcool/OMNIBus, which automatically starts the probe if it is down. If IBM Tivoli Netcool/OMNIBus is running, stop it before you start it. Run the following command to start IBM Tivoli Netcool/OMNIBus:

```
IOControl start ncob <password>
```

5. Verify that the service status of the EventProcessor, IOC_CAP_Event_Reader, and PolicyLogger is green. Use the Event Processing and Enhancing web-based console for Tivoli Netcool/Impact to verify the status. For information about how to open the IBM Intelligent Operations Center web-based administration consoles, see 3.3, “Administration Consoles” on page 55. See Figure 6-7 on page 146 for an example of the expected services status.
6. Verify that the event complies with the IOC_Event_Notification policy and that there are no policy violation messages in following log:

```
/opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Verify that the onset value for the incoming event is included. For example:

```
<onset>2012-07-25T15:59:05-00:00</onset>
```

Portal server

On the portal server, check whether a second user, with the same role, already acknowledged or closed the notification.

6.1.5 Correlated notification not displayed

Correlation flow: The troubleshooting process that is described in this section is driven by the IBM Intelligent Operations Center correlation flow. For information about the correlation flow, see 7.3, “Correlation flow” on page 203.

Events that are related by time, distance, and matching business rules are called *correlated events*. The time and distance of correlated events are configurable IBM Intelligent Operations Center system parameters, for example, within 5 miles or within 2 hours of time.

Correlated events are processed by business rules to determine if the values of the events fall out of the rule threshold. For those successfully processed events, a notification is generated and stored in the notification table and is related to other correlated events. This notification is displayed in the Notifications portlet with the correlated event information.

Correlated notifications: Most of the troubleshooting steps for correlated notifications that are not displayed are similar to and already detailed in 6.1.1, “Events that are not displayed in the Details portlet” on page 138. Reading 6.1.1, “Events that are not displayed in the Details portlet” on page 138 is a prerequisite to understanding the information in this section.

Example 6-10 shows a correlation notification XML message for two events that occurred close to each other.

Example 6-10 Sample correlation notification XML message

```
<?xml version="1.0" encoding="UTF-8" ?>
  <notification xmlns="urn:ibm:industry:solutions:ioc:notification:1.0">
    <notificationId>237443dc-71a3-4caa-a805-42b7b47fd171</notificationId>
    <notificationType>Alert</notificationType>
    <sentFrom>Correlation Engine</sentFrom>

    <sentToGroup>;CityWideExecutive;CityWideSupervisor;CityWideOperator;</sentToGroup>
    <headline>Possible correlation found</headline>
    <description>'Chemical Spill event' is possibly correlated with 'Wildfire
event' - The correlation was determined based on that target onset date less than
60 minutes after source onset date , target onset date less than 60 minutes before
source onset date , it's location intersects with a 5000 meter area around the
source event</description>

    <alertLink>d8b869f2-e823-4eec-8f76-aaf4a5fcf5da';'6b7df0ed-5218-4da8-945d-7246e43a
e653</alertLink>
    <kpiLink />
    <category>Transport</category>
  </notification>
```

Use the following sections to diagnose correlated event issues by logging in to the different servers with administration credentials and performing the steps for each server.

Application server

Complete the following steps on the application server:

1. Verify that all the services are running by checking the System Verification Check tool. For information about running System Verification Check tests, see 3.2, "System Verification Check" on page 48 more information.
2. Verify that the user is authorized to access the Notifications portlet. For details, see step 2 on page 140.
3. Verify that the Notifications portlet is visible on the Supervisor:Operations or Operator:Operations portal page.
4. Verify if the Notifications portlet is displaying other correlated notifications.
5. Verify that the incoming event corresponding to the missing notification is displayed in the Details portlet or the Map portlet. If the event is displayed, then the event was processed through the business rules.
6. Verify that there are no errors for the notification in the following portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Database server

Events are stored in the IOC.NOTIFICATION table under the db2inst1 instance. To check this table, complete the following steps on the database server:

1. Log in to the database server.

2. Run the following commands:

```
su - db2inst1
db2cc &
```

3. Select the IOC.NOTIFICATION table and display its contents.
4. If the notification is in the database and not on the portal server, ensure that the database is running by running the following command:

```
./IOCControl.sh status db24sol <password>
```

Event server

Complete the following steps on the event server:

1. Check that the queue manager IOC.MB.QM is running by checking it with WebSphere MQ Explorer. For information about using WebSphere MQ Explorer, see 3.6, “WebSphere MQ Explorer” on page 72.
2. Verify that the Current Queue Depth field has a value of 0 in the following queues:
 - IOC_JRULES_IN (also called IOC_JRULES_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY)
 - IOC_JRULES_OUT (also called IOC_JRULES_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY)
3. Verify that the Open Input Count field is greater than 0 in the IOC_JRULES_IN and IOC_JRULES_OUT queues.

If the Open Input Count field is 0 or if messages are increasing in the Current Queue Depth field, then restart the IBM WebSphere Operations Decision Manager application by running the following IOCControl commands:

```
./IOCControl.sh stop wodm <password>
./IOCControl.sh start wodm <password>
```

4. Check the following log files for errors:
 - /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - /opt/IBM/netcool/omnibus/log/NCOMS.log
 - /opt/IBM/netcool/omnibus/log/NCO_PA.log
 - /opt/IBM/netcool/impact/log/NCI_policylogger.log

Important: The `ioc_xml.log` file records the time stamp when the message was received from the external system, and the CAP format of the message with its event identifier. The `NCOMS.log` file records the duplicate events, if any. If the probe is down, the errors are logged in the `NCO_PA.log` file. The `NCI_policylogger.log` file displays the actual logged values as processed by the policy if the debug flag is on.

Example 6-11 gives a snapshot of the `ioc_xml.log` when the correlated events were logged.

Example 6-11 Sample of `ioc_xml.log` for correlated events

```
2012-07-25T16:11:31: Debug: D-JPR-000-000: Adding message from endpoint 'jms/ioc.notification.out.q' to
queue
2012-07-25T16:11:31: Debug: D-JPR-000-000: Received message from endpoint jms/ioc.notification.out.q: <?xml
version="1.0" encoding="UTF-8"?><notification
xmlns="urn:ibm:industry:solutions:ioc:notification:1.0"><notificationId>237443dc-71a3-4caa-a805-42b7b47fd17
1</notificationId><notificationType>Alert</notificationType><sentFrom>Correlation
Engine</sentFrom><sentToGroup>;CityWideExecutive;CityWideSupervisor;CityWideOperator;</sentToGroup><headlin
```

```

e>Possible correlation found</headline><description> 'test 2' is possibly correlated with 'test 1' - The
correlation was determined based on that target onset date less than 60 minutes after source onset date
, target onset date less than 60 minutes before source onset date
, it's location intersects with a 5000 meter area around the source
event</description><alertLink>d8b869f2-e823-4eec-8f76-aaf4a5fcf5da';'6b7df0ed-5218-4da8-945d-7246e43ae653</
alertLink><kpiLink></kpiLink><category>Transport</category></notification>
2012-07-25T16:11:31: Debug: D-JPR-000-000: Looking for transformer for endpoint: jms/ioc.notification.out.q
2012-07-25T16:11:31: Debug: D-JPR-000-000: Parsing transformed message:
notificationId:string:"237443dc-71a3-4caa-a805-42b7b47fd171"
notificationType:string:"Alert"
sentFrom:string:"Correlation Engine"
sentToGroup:string:";CityWideExecutive;CityWideSupervisor;CityWideOperator;"
headline:string:"Possible correlation found"
description:string:"'test 2' is possibly correlated with 'test 1' - The correlation was determined based on
that target onset date less than 60 minutes after source onset date , target onset date less than 60
minutes before source onset date , it's location intersects with a 5000 meter area around the source event"
alertLink:string:"d8b869f2-e823-4eec-8f76-aaf4a5fcf5da';'6b7df0ed-5218-4da8-945d-7246e43ae653"
kpiLink:string:""
category:string:"Transport"
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] TransformerName: notification2nvpairs
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] Endpoint: jms/ioc.notification.out.q
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] notificationId:
237443dc-71a3-4caa-a805-42b7b47fd171
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] notificationType: Alert
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] sentFrom: Correlation Engine
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] sentToGroup:
;CityWideExecutive;CityWideSupervisor;CityWideOperator;
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] headline: Possible correlation found
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] description: 'test 2' is possibly
correlated with 'test 1' - The correlation was determined based on that target onset date less than 60
minutes after source onset date , target onset date less than 60 minutes before source onset date , it's
location intersects with a 5000 meter area around the source event
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] alertLink:
d8b869f2-e823-4eec-8f76-aaf4a5fcf5da';'6b7df0ed-5218-4da8-945d-7246e43ae653
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] kpiLink:
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] category: Transport
2012-07-25T16:11:31: Debug: D-UNK-000-000: [Event Processor] Processing alert {0 remaining}
2012-07-25T16:11:31: Debug: D-UNK-000-000: <<<<< Entering... xml_notification.rules >>>>>
2012-07-25T16:11:31: Debug: D-UNK-000-000: Executing genevent() command for target server 'Notification'.
2012-07-25T16:11:31: Debug: D-UNK-000-000: genevent() created new alert for target server 'Notification'.
2012-07-25T16:11:31: Debug: D-UNK-000-000: genevent() created new alert for target server 'Notification'.
2012-07-25T16:11:31: Debug: D-UNK-000-000: genevent() sent new event to target server 'Notification'.
2012-07-25T16:11:31: Debug: D-UNK-000-000: <<<<< Leaving... xml_notification.rules >>>>>

```

5. Verify that the probe is running by running the following **IOControl** command on the management server:

```
IOControl status iocxml <password>
```

If the probe is off, restart it by starting IBM Tivoli Netcool/OMNIbus. Starting IBM Tivoli Netcool/OMNIbus automatically starts the probe if it is down. If IBM Tivoli

Netcool/OMNIbus is running, stop it before you start it by running the following command:

```
IOControl start ncoab <password>
```

6. Verify that the service status of the Event_Processor, IOC_CAP_Event_Reader, and PolicyLogger is green by checking them with the Event Processing and Enhancing web-based console. For details about opening the Event Processing and Enhancing console, see 3.3, "Administration Consoles" on page 55.

7. Verify that the event complies with the IOC_Event_Notification policy.
8. Ensure that the events published for correlation have the onset field populated in the message.

6.1.6 Resources are not being updated

Resource flow: The troubleshooting process that is described in this section is driven by the IBM Intelligent Operations Center resource flow. For information about the resource flow, see 7.5, “Resource flow” on page 211.

Every time a resource is created or updated, it follows the resource flow path that is described in 7.5, “Resource flow” on page 211. If resources are not being updated as expected, complete the steps in the following sections to troubleshoot the problem.

Before you begin: Before you complete the troubleshooting steps in this section, ensure that the user has access to the Details portlet and can see the Resources tab.

Application server

Complete the following steps on the application server:

1. Verify that all the services are running by using the System Verification Check tool. For more information about running System Verification Check tests, see 3.2, “System Verification Check” on page 48.
2. Verify that the Resources tab in the Details portlet is visible on the Supervisor:Operations or Operator:Operations portal page.
3. Confirm that the Resources tab is updating other resources.
4. Verify that the resource in question is geographically close to the event. To confirm this information, complete the following steps:
 - a. Log in to the IBM Intelligent Operations Center as an administrator (wpsadmin).
 - b. Go to the **Supervisor:Operations** or **Operator:Operations** page, click the **Details** portlet, click the **Events and Incidents** tab, and select an event.

Details portlet: In this troubleshooting scenario, the assumption is the events are displayed in the Details portlet.

- c. Right-click the event and select **View Nearby Resources** → **5 miles**. Figure 6-28 shows no resources within a 5-mile radius.

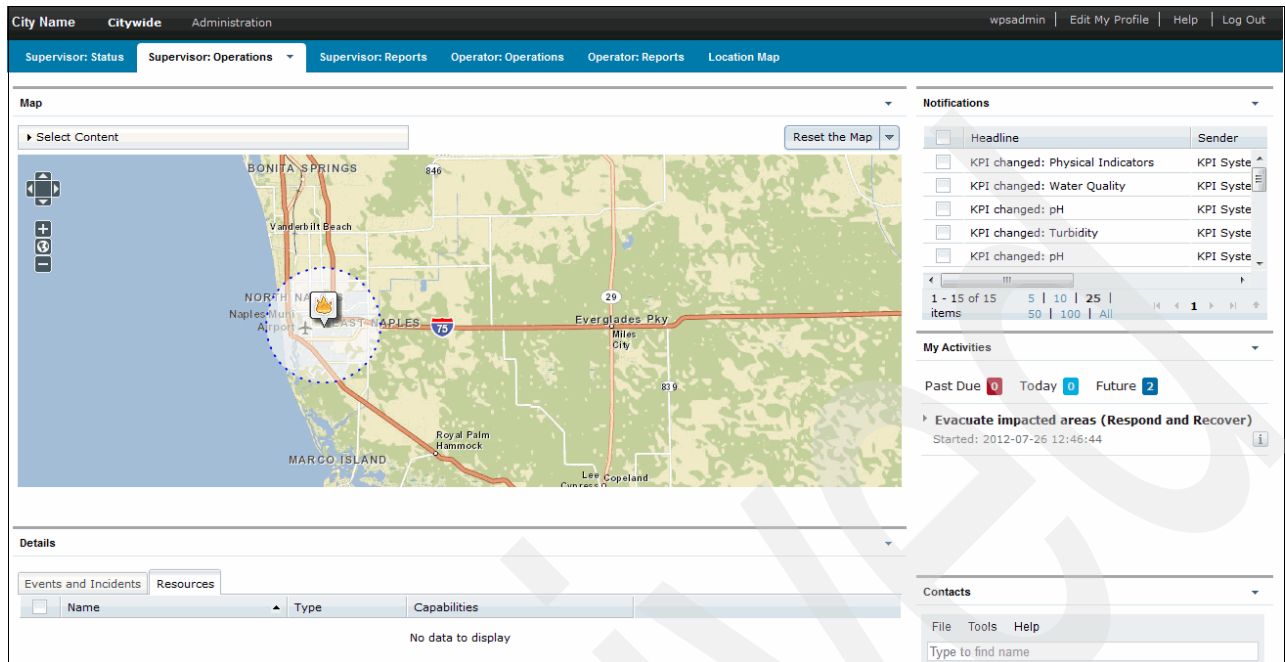


Figure 6-28 No resources within a 5-mile radius of the event

- d. If no resources are shown, right-click the event and select **View Nearby Resources** → **100 miles**. Figure 6-29 shows resources within the specified event range.

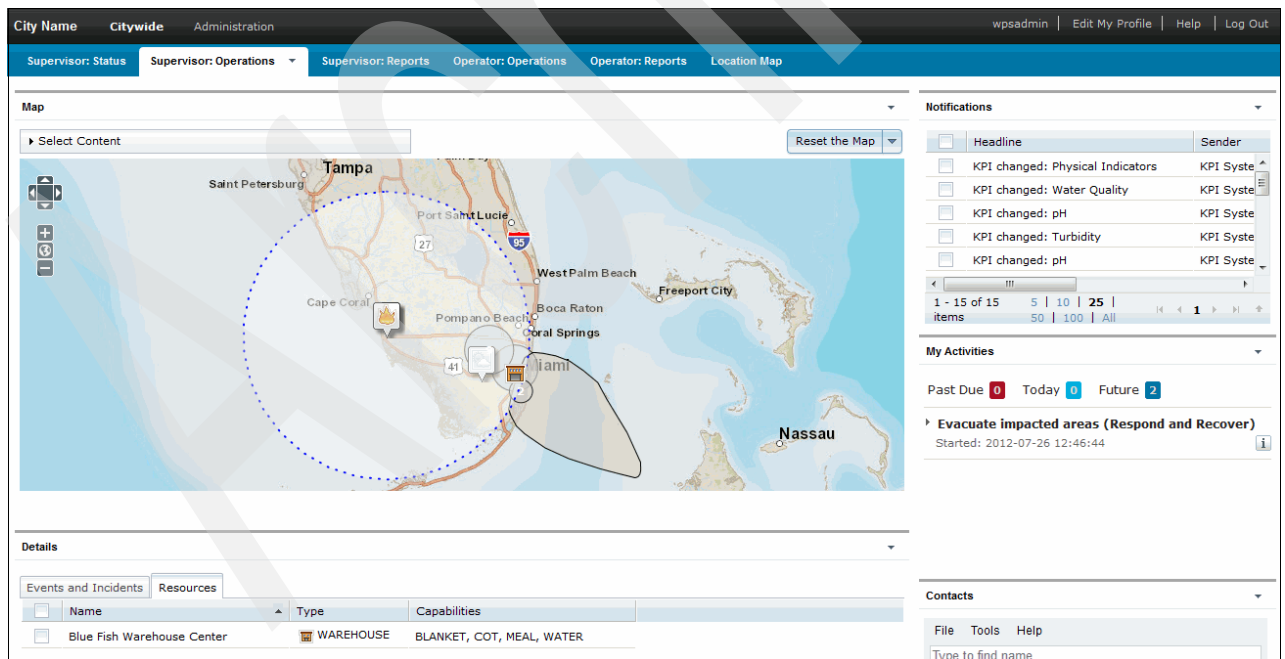


Figure 6-29 Resources found in a 100-mile radius of the event

5. Verify that the resource in question has capabilities that match the category of the event. To display the resources capabilities, complete the following steps:
 - a. Select the resource in the **Resources** tab.

- b. Expand **Select Content** in the Map portlet. Figure 6-30 shows the resources' capabilities.

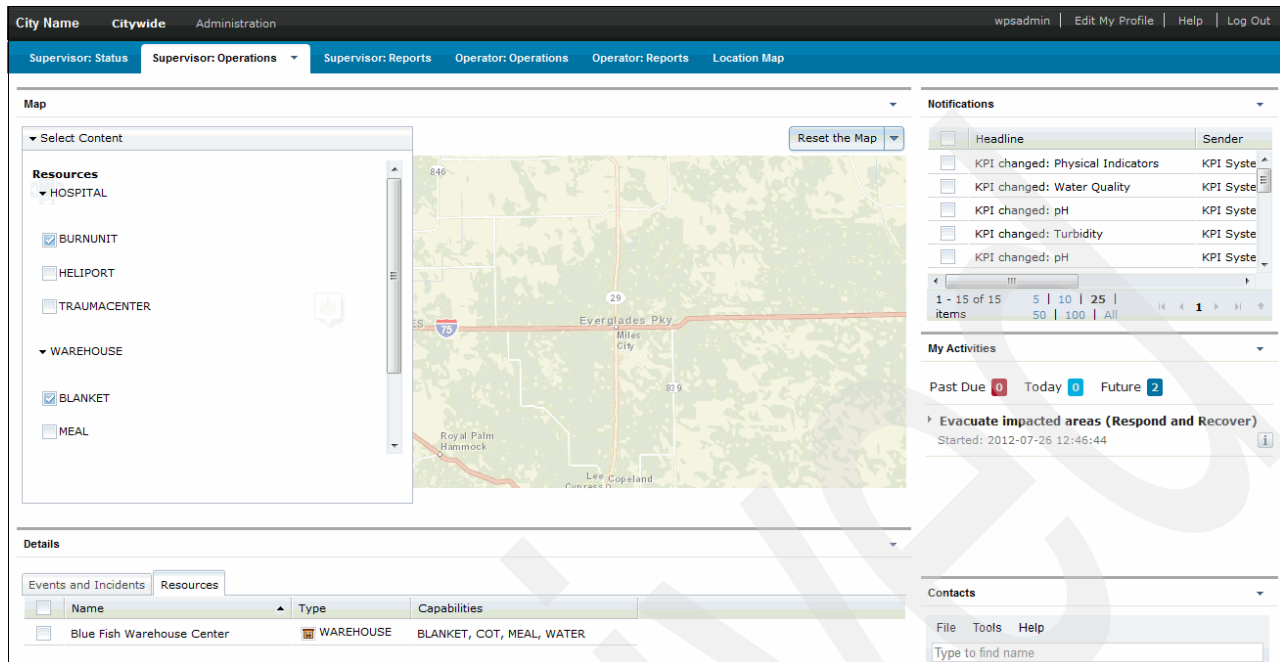


Figure 6-30 Resource capabilities

- Verify that there are no resources update errors in the following portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Database server

On the database server, verify that the resources are updated in the IOC.RESOURCE and IOC.RESOURCE_X_CAPABILITIES tables. Both of these tables are in the db2inst1 database.

Resources with successful updates are stored in the IOC.RESOURCE table with its capabilities mapped to the IOC.RESOURCE_X_CAPABILITY table. Complete the following steps to check these tables:

- Log in to the database server and run the following commands:


```
su - db2inst1
db2cc &
```

2. Verify that the contents of the Resource and the IOC.RESOURCE_X_CAPABILITY tables in the IOCDDB database are updated (Figure 6-31).

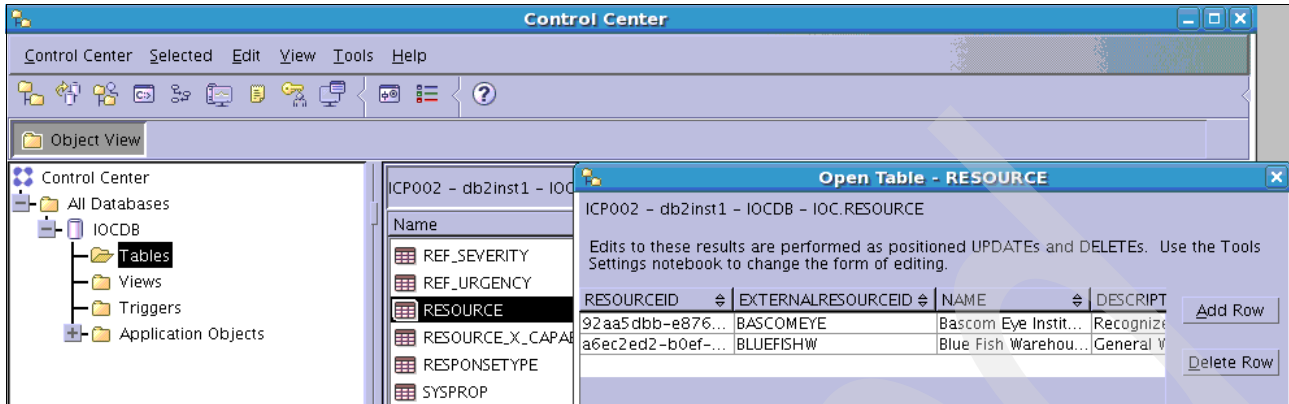


Figure 6-31 Displaying the content of the IOC.RESOURCE table

3. If the Resource table is populated but the resources are not displayed in the Details portlet, ensure that the data resources are active. To verify the data resource connection, complete the following steps:
 - a. Click **Administration Consoles** → **Application Server**, as described in 3.3, “Administration Consoles” on page 55.
 - b. Log in to the application server with administration authorities and click **Resources** → **JDBC** → **Data Sources**. (Figure 6-32).



Figure 6-32 Application server data sources

- c. Select **jdbc.ioc** from the list and click **Test connection**. Figure 6-33 shows a successful connection message.

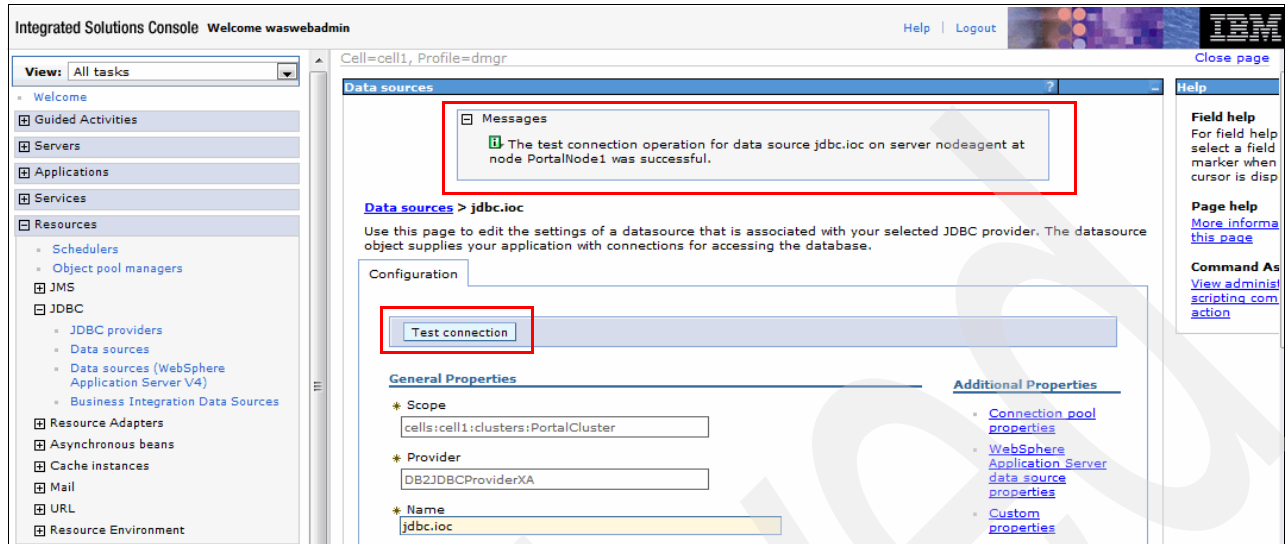


Figure 6-33 Testing a data source connection

4. Verify that the capabilities are updated in the IOC.CAPABILITY and IOC.CATEGORIES_X_CAPABILITY tables. Both tables are in the db2inst1 database. Figure 6-34 shows the contents of these tables.

Verify that the capabilities match the existing event categories.

Open Table - CAPABILITY			Open Table - CATEGORY_X_CAPABILITY	
ICP002 - db2inst1 - IOCDB - IOC.CAPABILITY			ICP002 - db2inst1 - IOCDB - IOC.CATEGORY_X_CAPABILITY	
Edits to these results are performed as positioned UPDATES and D Settings notebook to change the form of editing.			Edits to these results are performed as positioned UPDATES and DELETES. Use the Tools Settings notebook to change the form of editing.	
CAPABILITYID	NAME	DESCRIPTION	EVENTCATEGORY	CAPABILITYID
BIOLOGICAL	BIOLOGICAL	Biological	CBRNE	BIOLOGICAL
CHEMICAL	CHEMICAL	Chemical	Fire	BLANKET
SampleCapability	SampleCapability	This is a sample c...	Met	BLANKET
BLANKET	BLANKET	Has blankets	Fire	BURNUNIT
BURNUNIT	BURNUNIT	Has burn units	CBRNE	CHEMICAL
MEAL	MEAL	Has meals	Fire	COT
NUCLEAR	NUCLEAR	Nuclear	Met	COT
WATER	WATER	Has water	Safety	HELIPORT
COT	COT	Has cots	Met	MEAL
TRAUMACENTER	TRAUMACENTER	Has trauma center	Safety	MEAL
HELIPORT	HELIPORT	Has Heliport	CBRNE	NUCLEAR
			Env	SampleCapability
			Geo	SampleCapability
			Health	SampleCapability
			Infra	SampleCapability
			Other	SampleCapability
			Rescue	SampleCapability
			Security	SampleCapability
			Transport	SampleCapability
			Met	TRAUMACENTER
			Safety	TRAUMACENTER
			Met	WATER
			Safety	WATER

Figure 6-34 IOC.CAPABILITY and IOC.CATEGORY_X_CAPABILITY table contents

Event server

Complete the following steps on the event server:

1. Check that the queue manager IOC.MB.QM by checking it with WebSphere MQ Explorer. For more information about using WebSphere MQ Explorer, see 3.6, “WebSphere MQ Explorer” on page 72.
2. Verify that the Current Queue Depth field has a value of 0 in the IOC_RESOURCE_IN and IOC_RESOURCE_OUT queues.
3. Check whether there are any errors in the following log files:
 - /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - /opt/IBM/netcool/omnibus/log/NCOMS.log
 - /opt/IBM/netcool/omnibus/log/NCO_PA.log
 - /opt/IBM/netcool/impact/log/NCI_policylogger.log

Important: The `ioc_xml.log` file records the time stamp when the message was received from the external system, and the CAP format of the message with its event identifier. The `NCOMS.log` file records the duplicate events, if any. If the probe is down, the errors are logged in the `NCO_PA.log` file. The `NCI_policylogger.log` file displays the actual logged values as processed by the policy if the debug flag is on.

4. Verify that the probe is running by running the following **IOControl** command on the management servers:

```
IOControl status iocxml <password>
```

If the probe is off, restart it by starting IBM Tivoli Netcool/OMNIBus. Starting IBM Tivoli Netcool/OMNIBus automatically starts the probe if it is down. If IBM Tivoli Netcool/OMNIBus is running, stop it before you start it by running the following command:

```
IOControl start ncob <password>
```
5. Verify that the service status of the Event_Processor, IOC_CAP_Event_Reader, and PolicyLogger is green by using the Event Processing and Enhancing web-based console. For details about opening the Event Processing and Enhancing console, see 3.3, “Administration Consoles” on page 55.
6. Verify that the event complies with the IOC_Event_Resource policy.

6.1.7 Event Publisher tool not publishing events on the Details portlet

The Event Publisher tool in IBM Intelligent Operations Center provides sample data and an interface to publish events, KPIs, and correlated events. The sample events are displayed in the Details and Map portlets.

If events are not displayed on the Details or Map portlets, verify the following settings in the XML message that is generated by the tool:

- ▶ The `sent` element contains the current time stamp. For example:

```
<sent>2012-03-26T15:58:21-00:00</sent>
```
- ▶ The time stamp in the `onset` element is the same as the `sent` element or later. For example:


```
<onset>2012-03-26T16:10:21-00:00</onset>
```
- ▶ The `code` element contains the value `Event`.

- ▶ The latitude and longitude positions are set correctly under the area element. Here is an example of the position information:

```
<circle>25.92725,-80.21736 0</circle>
```

6.1.8 Unable to log in to the IBM Intelligent Operations Center

In this scenario, a user attempts to log in to the IBM Intelligent Operations Center and is unsuccessful, with error “HPDIA0119W: Authentication mechanism is not available”, as shown in Figure 6-35.



The screenshot shows a login page for the IBM Intelligent Operations Center. At the top, it says "City Name" followed by a horizontal line. Below that is the title "Intelligent Operations Center". There are two input fields: "User ID:" and "Password:". Below the password field is a note: "Please note, after some time of inactivity, the system will sign you out automatically and ask you to sign in again." There is a "Sign In" button. At the bottom, there is a copyright notice: "Licensed Materials - Property of IBM Corp, IBM Corporation and other(s) 2011,2012. IBM is a registered trademark of IBM Corporation, in the United States, other countries, or both." A red error message is displayed at the bottom: "HPDIA0119W Authentication mechanism is not available."

Figure 6-35 IBM Intelligent Operations Center login failure message

To troubleshoot this problem, complete the following steps:

1. Verify that there are no login errors in the following portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
2. Verify that the directory service is running. Run the following **IOCControl** command to first check the status and then restart the service if not running:

```
./IOCControl.sh status tds <password>
```

If the output of the command is the following:

```
Executing query command...completed.  
IBM Tivoli Directory Server [ Off ]  
Command completed successfully
```

Then, restart the directory service by running the following command:

```
./IOCControl.sh start tds <password>
```

3. If the user was recently added or imported to the directory, but not through the IBM Intelligent Operations Center user management interface, verify that the user is associated with the management policy database. For more information, see 5.1.6, “Importing users from a user registry” on page 109.

6.1.9 Login shows “Third-party server not responding” error message

The “Third-party server not responding” error message is usually displayed when the portal service is stopped and the access management service is running. Figure 6-36 shows the error as it displayed when a user tries to log in.

Third-party server not responding.

The resource you have requested is located on a third-party server. WebSEAL has attempted to send your request to that server, but it is not responding.

Explanation

This could be due to the third-party server being offline, or to network problems making it unreachable. The problem is not with the WebSEAL server itself.

Solutions

Retry your request later, or contact the system administrator for assistance.

Figure 6-36 Third-party server not responding on login

Verify that the portal service is running by running the following **IOCControl** command:

```
./IOCControl.sh status wpe <password>
```

Restart the portal service if it is stopped by running the following **IOCControl** command:

```
./IOCControl.sh start wpe <password>
```

6.1.10 Cannot access the login window

In this scenario, the user is unable to see the login window. The most likely reason for this problem is that the access service stopped. To troubleshoot and recover from this issue, complete the following steps:

1. Verify the status of the access service by running the following **IOCControl** command:

```
./IOCControl.sh status tamweb <password>
```

Here is the output of the command:

```
Executing query command...completed.  
IBM Tivoli Access Manager WebSEAL [ off ]  
Command completed successfully
```

2. If the status of IBM Tivoli Access Manager WebSEAL is off, start it by running the following **IOCControl** command:

```
./IOCControl.sh start tamweb <password>
```

6.1.11 Portlets error “An error has occurred communicating with the servers”

Figure 6-37 shows a dialog box that is displayed when you navigate through the IBM Intelligent Operations Center portlets. This error is displayed when the session times out.

To correct this issue, do one of the following actions:

- ▶ Refresh the web browser page or log in to the IBM Intelligent Operations Center again.
- ▶ Verify that all the services are running by checking them through the System Verification Check tool. For more information about running System Verification Check tests, see 3.2, “System Verification Check” on page 48.



Figure 6-37 Connection error dialog box

6.1.12 User login expired error

The user login expired error normally occurs when the user password is expired. Figure 6-38 shows the error when the password is expired. To recover from this issue, provide the new password.

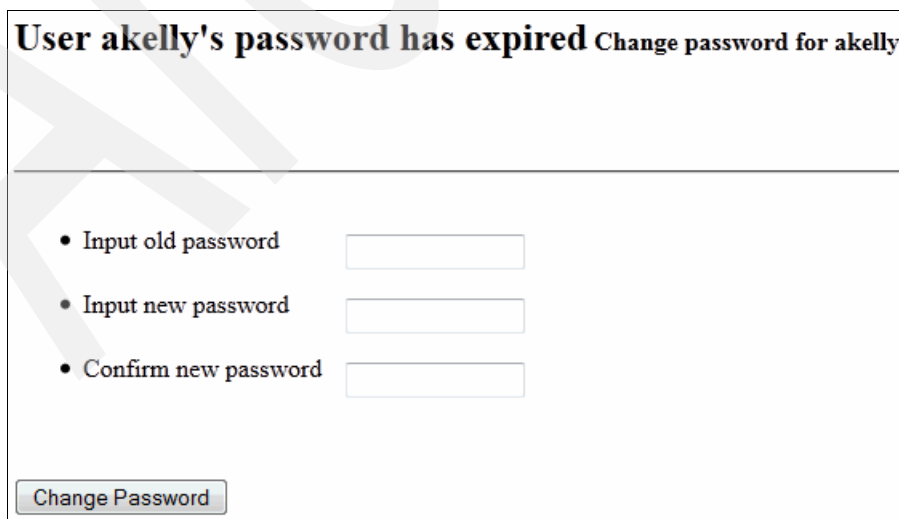


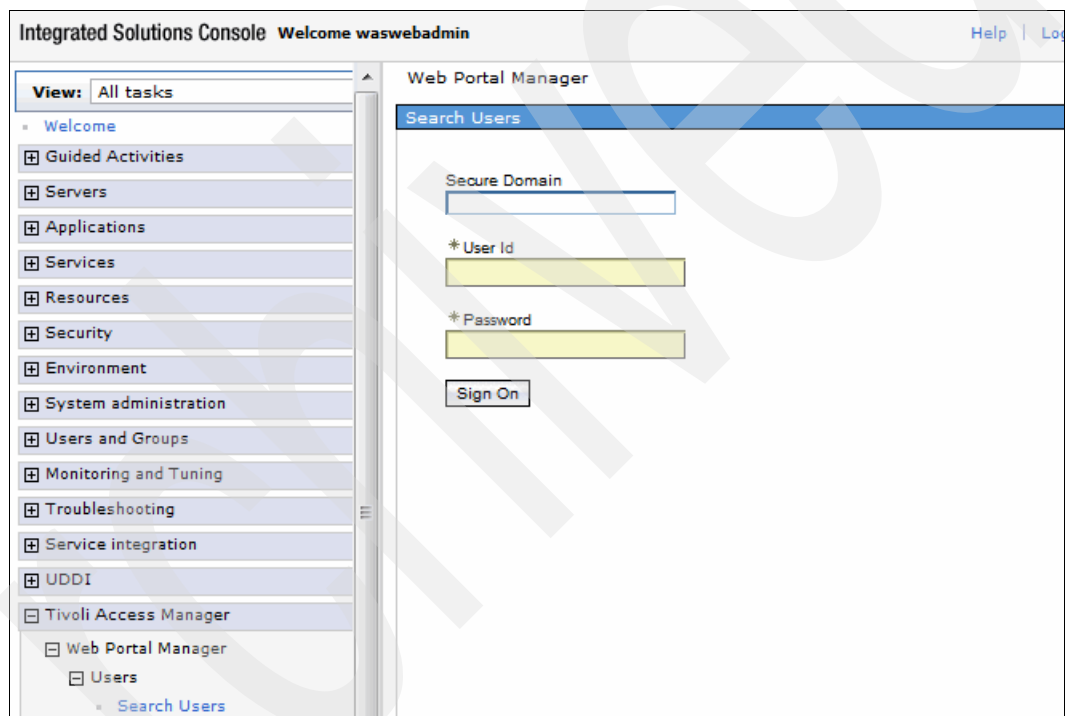
Figure 6-38 User password expired error

6.1.13 Login shows the “Error 403: Authentication Failed” error

The login error “Error 403: Authentication Failed” occurs when the IBM Intelligent Operations Center internal account password is expired.

To correct this issue from the application server administration console, complete the following steps:

1. Log in to the Application Server for Management -based console under the Management server. For more information about starting web consoles, see 3.3, “Administration Consoles” on page 55.
2. Click **Tivoli Access Manager** → **Web Portal Manager** → **Users** → **Search Users**. Figure 6-39 shows the user authentication form.
3. Log in to the Web Portal Manager with user ID `sec_master` and the password. Click **Sign On**.



The screenshot displays the Integrated Solutions Console interface. The top navigation bar includes the text "Integrated Solutions Console Welcome waswebadmin" and links for "Help" and "Log". A left-hand navigation pane shows a tree view with categories like "Guided Activities", "Servers", "Applications", "Services", "Resources", "Security", "Environment", "System administration", "Users and Groups", "Monitoring and Tuning", "Troubleshooting", "Service integration", "UDDI", "Tivoli Access Manager", "Web Portal Manager", and "Users". The "Search Users" option under "Users" is selected. The main content area, titled "Web Portal Manager", contains a "Search Users" section with the following fields: "Secure Domain" (text input), "* User Id" (text input with a yellow background), and "* Password" (text input with a yellow background). A "Sign On" button is located below these fields.

Figure 6-39 User authentication form

4. On the Search Users window, click **Search**. Figure 6-40 shows the list of accounts.

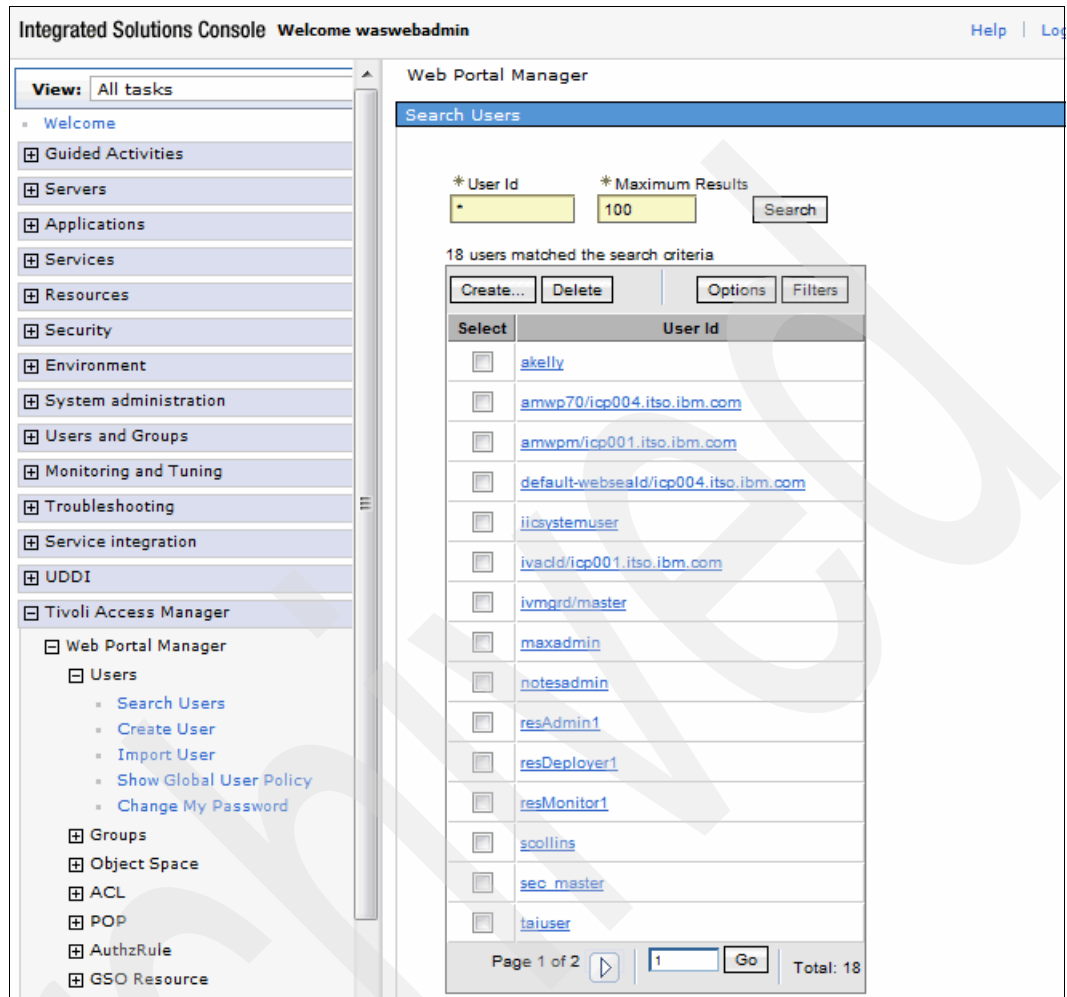


Figure 6-40 List of IBM Intelligent Operations Center user accounts

5. Select **taiuser** from the list of accounts.
6. Click the **Policy** tab for taiuser.

- In the Max Password Age section, click **Set** and provide the required time frame for the next password expiration. Figure 6-41 shows the policy form for taiuser.

Password expiration: If the time provided in the Max Password Age setting is set to 0, then the password never expires.

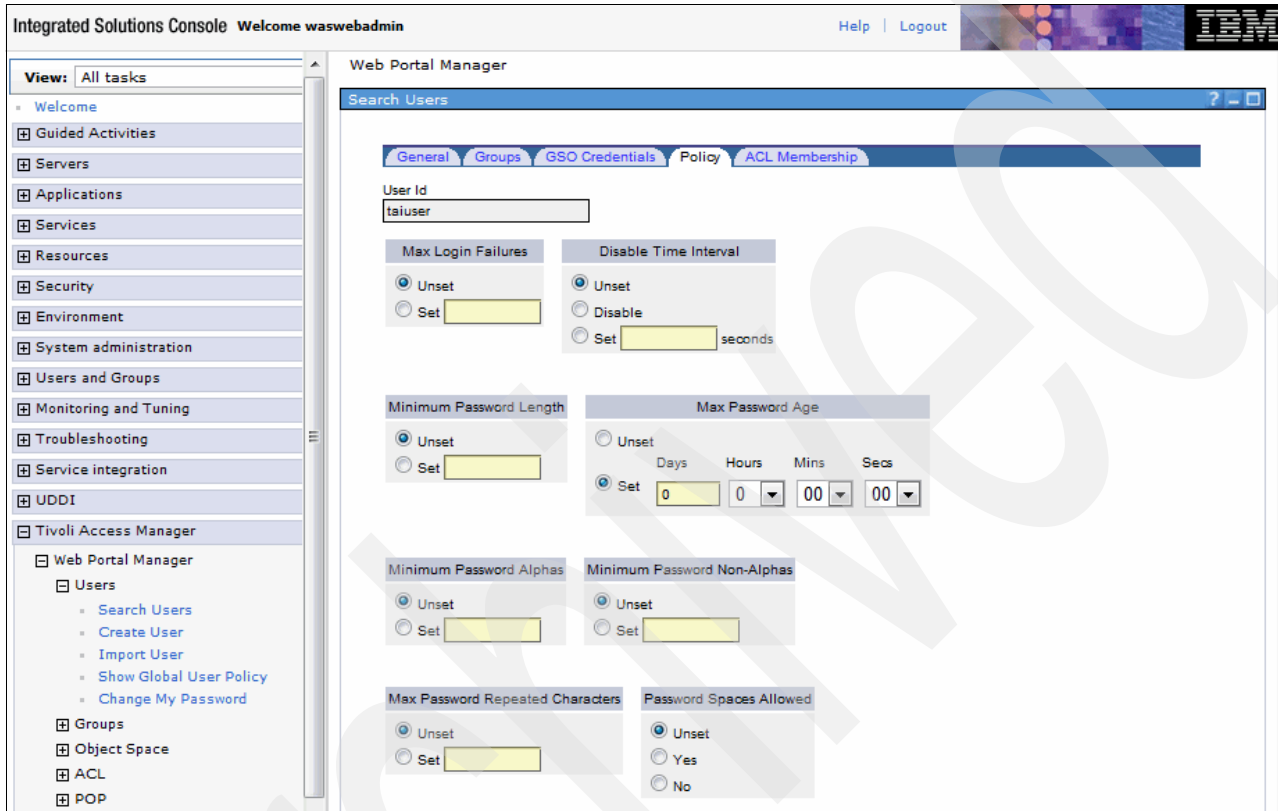


Figure 6-41 Policy options for taiuser

6.1.14 Portal shows the error message “There is no content available”

The error message “There is no content available” (Figure 6-42) usually appears when the user is created, but is not assigned to any groups and therefore has no access to portal resources.

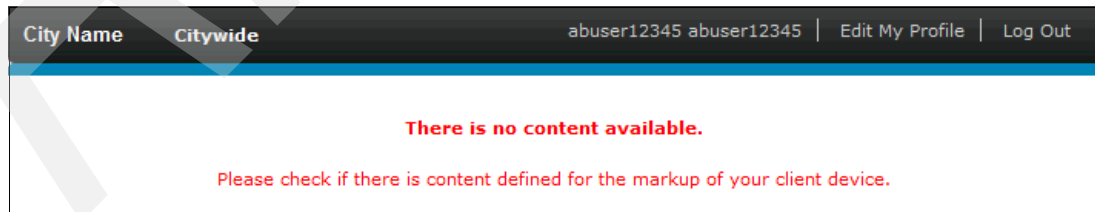


Figure 6-42 No content available error

To recover from this error, log in to the portal as an administrator.

For information about granting users permissions to access portal resources, see 5.2.2, “Portal resource permissions and user role groups” on page 111.

6.1.15 Portlets on the IBM Intelligent Operations Center page are closed

IBM Intelligent Operations Center portlets require web browsers with the JavaScript option running. Figure 6-43 shows when the portlet appears to be in closed state.

Verify that the web browser used to view the IBM Intelligent Operations Center portlet allows JavaScript to run for all the sites that are checked.

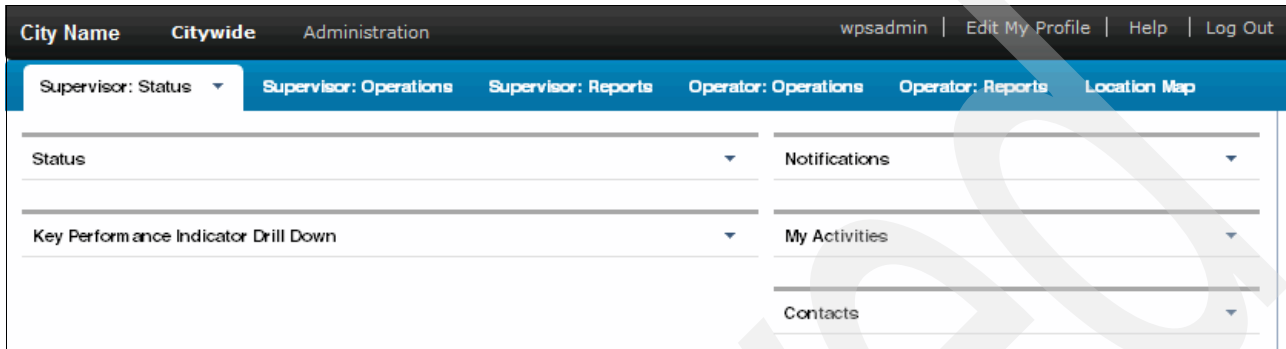


Figure 6-43 Portlets not visible in the IBM Intelligent Operations Center

6.1.16 Contacts portlet prompts for user name and password

In this scenario, the Contacts portlet where the authorized users are listed is not shown. Instead, a login portlet is displayed (Figure 6-44).

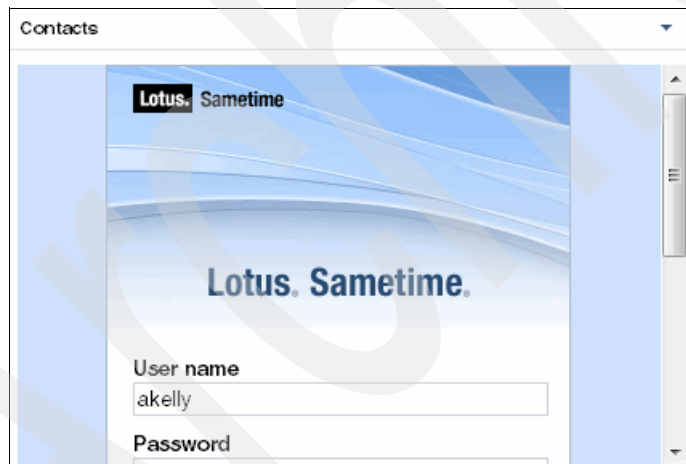


Figure 6-44 Contact login portlet

To troubleshoot this problem, complete the following steps:

1. Verify that the portlet page is refreshed.
2. Verify that the web browser cache is cleared.
3. Log out of the IBM Intelligent Operations Center and log back in.

If the user is unable to log back in to the IBM Intelligent Operations Center, then the directory that holds the LDAP services is in a busy state. To correct this situation, complete the following steps:

- a. Restart the directory service by running the following **IOCControl** commands:

```
./IOCControl.sh stop tds <password>
./IOCControl.sh start tds <password>
```
- b. Restart the collaboration services and portal in that order with the following **IOCControl** commands:

```
./IOCControl.sh stop wpe <password>
./IOCControl.sh stop st <password>
./IOCControl.sh start st <password>
./IOCControl.sh start wpe <password>
```

6.1.17 The Cognos Report page shows a server error

The Cognos Report in the IBM Intelligent Operations Center shows reports that are associated with the solution. Figure 6-45 shows the error when the Cognos Report portlet is not displayed. This situation is normally the case when the Cognos service is not running and the portal service is running.



Figure 6-45 Cognos portlet error

To correct this error, restart the Cognos service. Run the following **IOCControl** commands:

```
./IOCControl.sh stop cognos <password>
./IOCControl.sh start cognos <password>
```


6.1.18 The KPI portlet is not refreshing the status

The IBM Intelligent Operations Center has system properties for KPI caching. Verify that the system properties `CacheKpis` and `KpiCacheRefreshInterval` are properly set:

- ▶ If the variable `CacheKpis` is set to `true`, then the KPI status is refreshed according to the time set in `KpiCacheRefreshInterval`.
- ▶ If the variable `CacheKpis` is set to `false`, then the KPI is refreshed instantly.

For more details about IBM Intelligent Operations Center system properties, see 3.10, “System-wide configuration properties” on page 80.

If the system properties `CacheKpis` and `KpiCacheRefreshInterval` are properly set and the problem persists, see 6.1.3, “KPIs not displayed in the Status or Drill Down portlets” on page 155.

6.1.19 IBM Intelligent Operations Center page loads slowly

A system slowdown normally occurs when the server’s processor usage is high. For guidance about how to verify the processor usage of the IBM Intelligent Operations Center servers, see 3.5, “System monitoring” on page 65.

6.2 Troubleshooting resources and references

This section provides information about several support options that are provided by IBM to help you with various problem determination needs. For information about collecting problem data and inspecting logs, see 3.9, “MustGather tool” on page 78.

6.2.1 IBM Support portal

The IBM Support portal is an integrated view of all IBM technical support tools, resources, and information. In the Support portal, you have access to updated content and feeds. Other various support-related resources, such as flashes and news alerts, subscribed notifications, contact support, and self-assessment tools, are also available.

The IBM Support Portal can be found at the following website:

http://www-947.ibm.com/support/entry/portal/overview/software/smarter_cities/ibm_intelligent_operations_center

6.2.2 IBM Service Request tool

You can use the IBM Service Request tool to create service requests from a web browser. Here is the link to the IBM Service Request tool (you must be registered to use it):

https://www-947.ibm.com/support/entry/myportal/open_service_request/software/software_support_%28general%29

6.2.3 IBM Support Assistant

The IBM Support Assistant is a no cost software add-on that you can use to help diagnose problems by collecting data, such as log and trace files, automatically. This automation process can help you identify issues rapidly and reliably with little effort, assist you with performing self analysis, and discover solutions in a short amount of time.

For more information or to download the IBM Support Assistant, visit the IBM Support Center at:

<http://www-01.ibm.com/software/support/isa/>

Data flows

There are several data flows that represent the flow of data through the IBM Intelligent Operations Center topology. It is important to understand these flows, as they provide an end-to-end view of the paths traveled by the data for key IBM Intelligent Operations Center functions. Administrators can use these data flows to understand normal operations and also to help debug problems. Topics that are covered in this chapter include:

- ▶ Event flow
- ▶ Key performance indicators flow
- ▶ Correlation flow
- ▶ Notification flow
- ▶ Resource flow
- ▶ User authentication and authorization flow
- ▶ Overall system flows

Queue names: The queue names are shortened in the following sections to improve readability. Table 7-1 shows the full and corresponding short queue names.

Table 7-1 Full and short queue names

Full queue name	Short queue name
IOC_CAP_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_CAP_OUT
IOC_JRULES_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_JRULES_IN
IOC_JRULES_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_JRULES_OUT
IOC_KPI_IN_INTERNAL_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_KPI_IN
IOC_KPI_OUT_INTERNAL_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_KPI_OUT
IOC_KPI_UPDATE_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_KPI_UPDATE
IOC_NOTIFICATION_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_NOTIFICATION_IN
IOC_NOTIFICATION_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_NOTIFICATION_OUT
IOC_RESOURCE_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_RESOURCE_IN
IOC_RESOURCE_OUT_INTERNAL_USE_ONLY_DO_NOT_MODIFY	IOC_RESOURCE_OUT

7.1 Event flow

One of the main purposes of the IBM Intelligent Operations Center is to monitor relevant situations and provide operators with visibility of these situations, alerting them to impending emergencies. This information can then be used to ensure that the appropriate response actions are performed efficiently and in a timely manner. Therefore, the ability to receive information about these situations, process, and display it to operators in near real time is of the utmost importance.

Monitoring of situations in IBM Intelligent Operations Center is done by receiving events in the form of XML messages. These events contain information about the nature and category of the situation. The event flow that is presented in this section describes how these XML messages are received by the system and how they are processed, stored in the database, and displayed to operators in the user interface.

Figure 7-1 shows the event flow.

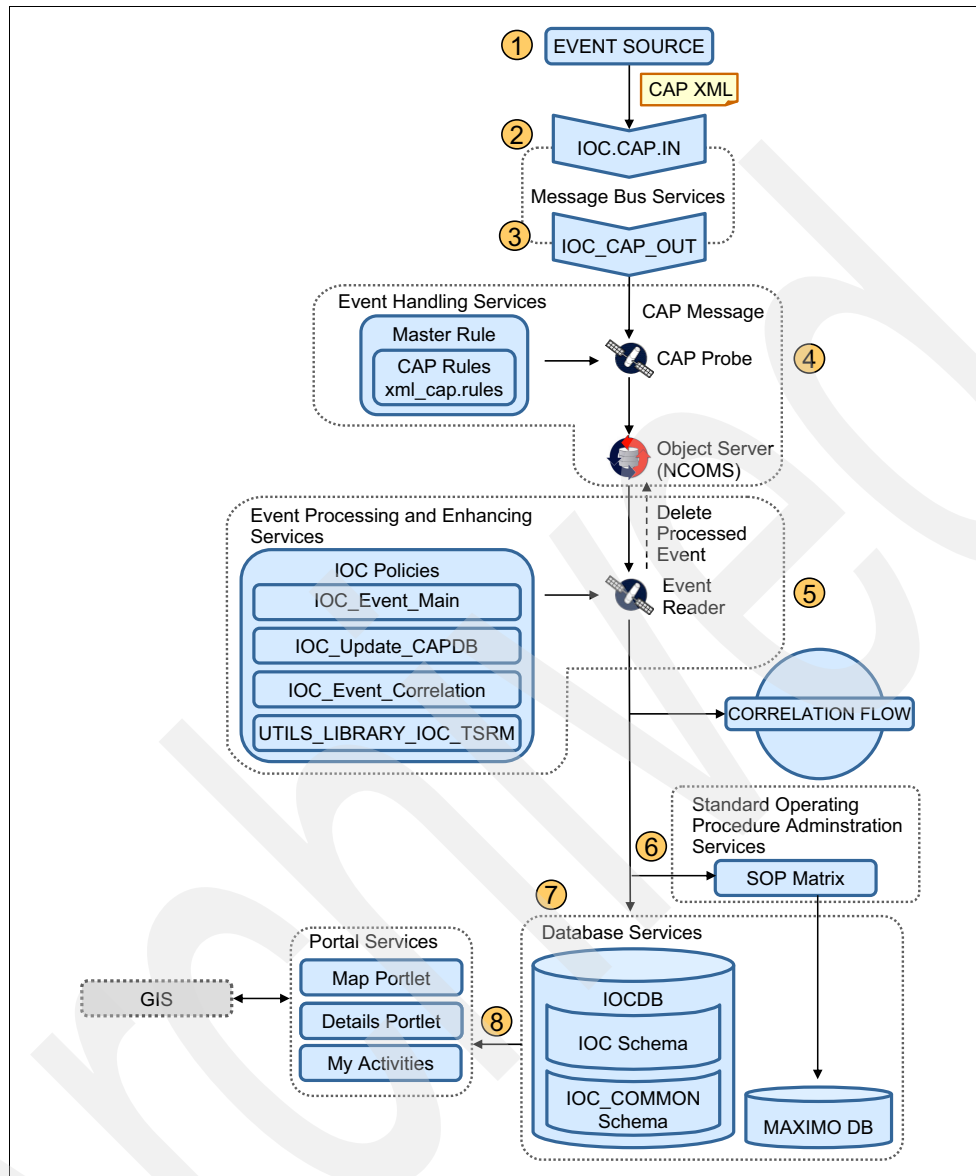


Figure 7-1 Event flow

The following steps correspond to the event flow steps shown in Figure 7-1:

1. An event source sends a CAP event message to the system. The event source can be:
 - An external source
 - The sample event portlet
 - An event that is created directly in the Map portlet

CAP messages: A CAP message is an XML message in the Common Alerting Protocol format, which is an open standard. The specifications for the CAP format can be found at the following website:

<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>

2. The message comes into the system through an input queue. This queue is part of the messaging handling service.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Messaging handling
- Input queue name: IOC.CAP.IN
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Platform Control tool (**IOControl**): Used to verify the status and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```
- Logs:
 - /var/mqm/errors/AMQERR*.LOG
 - /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the input queue are an indication that the messaging services is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** command.

3. The messaging bus takes the message from the input queue and puts it in the output queue.

Here are the various touch points for this step:

- Service location: Event server
- Services names: Messaging handling and message bus
- Output queue name: IOC_CAP_OUT
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)

Messaging (WebSphere Message Queue Publish/Subscribe topic)

- Platform Control tool (**IOCControl**): Used to verify and manage selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status wmb <password>
```

- Logs:

- /var/mqm/errors/AMQERR*.LOG
- /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the output queue are an indication that the CAP probe is down. Run the System Verification Check tool to verify if the event handling services are running or restart the services with the **IOCControl** tool.

4. The CAP XML probe gets the message from the IOC_CAP_OUT queue and processes the message using rules. The probe uses a master rule that calls a CAP rule definition file. The XML CAP message is decomposed and put in to the correct tables in the Object Server NCOMS database. If the probe is able to process the message successfully, it is placed in the Object Server NCOMS database; otherwise, the message is discarded.

Probes: Probes are software agents that monitor and capture data from different sources and forward them to the Object Server NCOMS database. The data can be treated by applying predefined rules to them, allowing filtering, deduplication, and other operations. Each probe type acquires data from a specific source.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event handling
- Probe name: CAP
- Administration tools:
 - System Verification Check tool: Used to check the status of the event handling services. The Monitoring (Tivoli Netcool/OMNIbus) test can be run to verify whether this service is running
 - **IOCControl** tool: Used to verify and to start or stop selected services. The following commands can be used to query the status of the event handling services:
Tivoli Netcool/OMNIbus process:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status ncob <password>
```


Tivoli Netcool/OMNIbus probes:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status iocxml <password>
```
 - Object Server NCOMS database configuration tool: Used to verify the NCOMS database status. The relevant command is:

```
/opt/IBM/netcool/omnibus/bin/nco_config
```
- Logs:
 - Probe log: /opt/IBM/netcool/omnibus/log/ioc_xml.log
 - Object Server NCOMS database log: /opt/IBM/netcool/omnibus/log/NCOMS.log

Messages accumulating in the Object Server NCOMS database are an indication that the event reader is not able to process messages in timely manner. Verify if the event processing and enhancing services are running.

Important: If messages are not showing up in the Object Server NCOMS database, it might be because they are failing the CAP rule check that is performed by the probe. Make sure that the message is in the correct CAP format.

5. The Object Server NCOMS database informs the event reader to pick up the message. The event reader is a service that runs in the event server. It processes the message according to the defined policies.

The main policy, called IOC_Event_Main, invokes the other policies. The IOC_Update_CAPDB policy processes the message, decomposing it, and updating the IBM Intelligent Operations Center database. It also invokes the UTILS_LIBRARY_IOC_TSRM policy, which sends the information about the event to the standard operating procedure administration service. The IOC_Event_Correlation policy triggers the correlation flow to every event that is read from the Object Server NCOMS database. For information about the correlation flow, see 7.3, “Correlation flow” on page 203.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event processing and enhancing
- Event reader service name: IOC_CAP_Event_Reader

Event readers: Event readers are services that query events in data sources at some defined intervals and then apply defined policies to the event data.

- Policies names:
 - IOC_Event_Main.
 - IOC_Update_CAPDB.
 - IOC_Event_Correlation.
 - UTILS_LIBRARY_IOC_TSRM.
- Administration tools:
 - System Verification Check tool: Used to check the status of the event processing and enhancing services. The Monitoring (Tivoli Netcool/Impact Console) test can be run to verify if this service is running.
 - **IOCControl** tool: Used to verify and manage selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status nci <password>
```
 - Administration consoles: Event Processing and Enhancing (web-based console for Tivoli Netcool/Impact)
- Policies log: /opt/IBM/netcool/impact/log/NCI_policylogger.log

6. The standard operating procedure administration server monitors updates to the IOCDB database. For every new event in the database, it checks its characteristics against the Standard Operating Procedures (SOP) matrix, which maps event characteristics to specific procedures. If the event matches one of the defined situations in the matrix, a new standard operating procedure workflow is initiated and is visible in the My Activities portlet.

Here are the various touch points for this step:

- Service location: Event server and application server
- Services names:
 - Standard operating procedure administration in the event server
 - Portal in the application server
- Portlets name: My Activities portlet
- Administration tools:
 - System Verification Check tool: Used to check the status of the standard operating procedure administration services. The Policy (IBM Tivoli Service Request Manager Maximo® Console) test can be run to verify whether this service is running.
 - Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the standard operating procedure administration services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status tsrm <password>
```
 - Administration Consoles:
 - Standard Operating Procedure Administration (web-based console for Tivoli Service Request Manager Start Center)
 - Standard Operating Procedure Application Server (web-based console for Web Application Server, which serves Tivoli Service Request Manager)
- Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

7. The event reader applies the defined policies and then the Netcool/Impact server writes the decomposed message to the IOCDB database, updating two different schemas: IOC and IOC_COMMON. When it completes writing the data in the database, the message is deleted from the Object Server NCOMS database.

Here are the various touch points for this step:

- Service location: Data server
- Service name: Database
- Database instance: db2inst1
- Database name: IOCDB
 - Database schemas names: IOC and IOC_COMMON
 - Main database tables affected: IOC.CAPALERT and IOC_COMMON.EVENT
- Administration tools:
 - System Verification Check tool: Used to check the status of the database services. The following tests can be run to verify if this service is running:
Database (DB2 Instance - db2inst1)
Database (DB2)

- Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db2sol <password>
```

- DB2 Control Center: db2cc as db2inst1 user
- Database log: /datahome/db2inst1/sqllib/log

8. The event update servlet notifies the data provider that updates are available for users. Event data providers are the portlets responsible for the presentation of the user interface. The event data provider retrieves the latest data from the database and updates the user interface. The Map portlet interacts with the GIS system to obtain the map information.

Here are the various touch points for this step:

- Service location: Application server
- Service name: Portal
- EAR names (applications that should be running in the application server):
 - ioc_portal_ear
 - iss_curi_ear
 - iss_help_war
 - iss_portal_ear
- Portlets names:
 - Map portlet
 - Details portlet
- Administration tools:
 - Platform Control tool (**IOControl**): The following command can be used to query the status of the portal services:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wpe <password>
```
 - Administration consoles: Used to check the status of the portal services. The Application Server (web-based console for WebSphere Application Server) test can be run to verify if this service is running.
- Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

Important: The GIS system is external to the IBM Intelligent Operations Center solution. If the GIS system is down, map information is not available. Verify that the GIS service is running and available for the IBM Intelligent Operations Center.

7.2 Key performance indicators flow

A key performance indicator (KPI) for the IBM Intelligent Operations Center is a CAP message that contains indicator information and is identified by a specific code in the CAP message. It is used for status reporting and monitoring for status changes. KPIs can be used to summarize the status of different domains to executives or supervisors and allow drilling down into the KPI details for further investigation.

The KPI flow is similar to the event flow, with some additional steps to process the KPI.

Figure 7-2 shows the KPI flow.

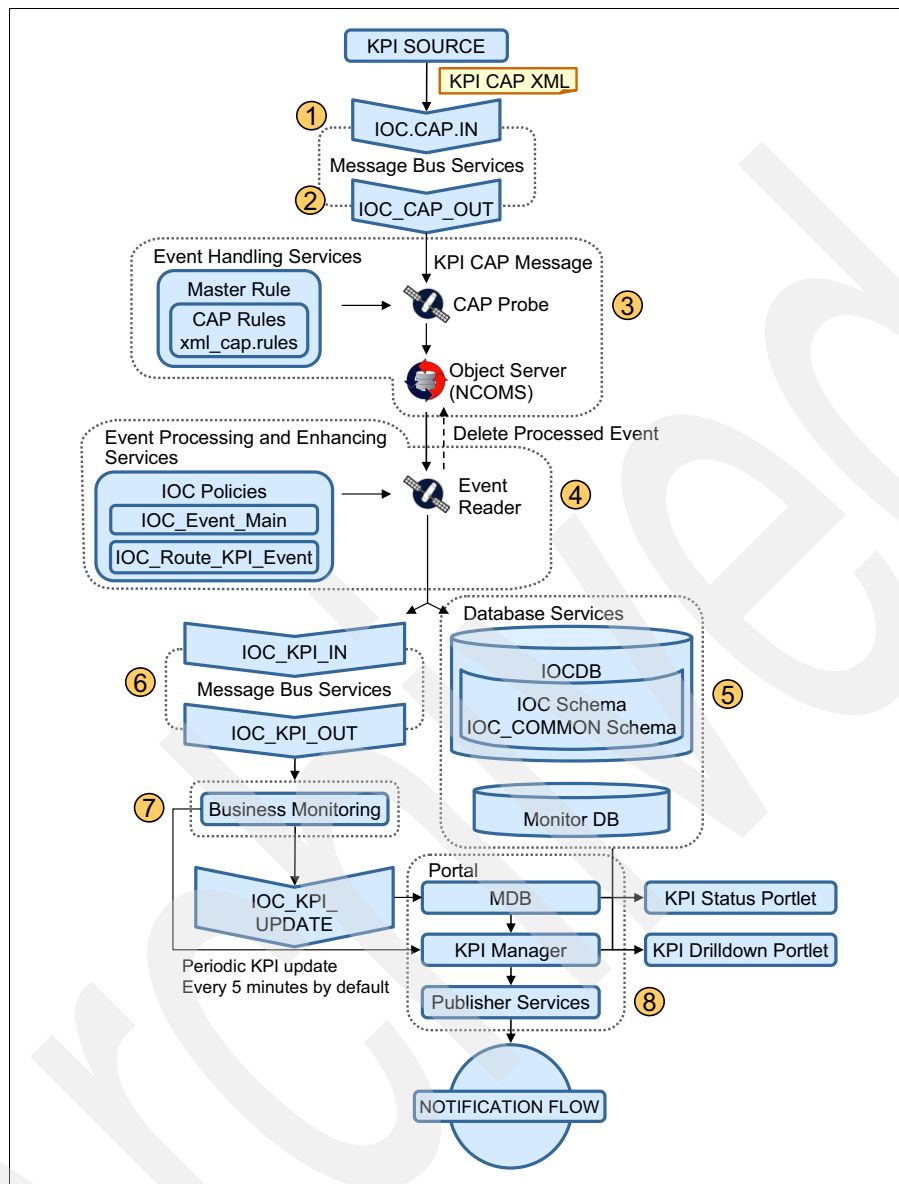


Figure 7-2 KPI flow

The following steps correspond to the KPI flow steps shown in Figure 7-2:

1. A KPI source sends a KPI CAP message to the system. The KPI source can be an external system or the event publisher tool that is used for testing and troubleshooting.

CAP message: A CAP message is an XML message in the Common Alerting Protocol format, which is an open standard. The specifications for the CAP format can be found at the following website:

<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>

The KPI CAP message must have the code KPI in the field cap:code:

```
<cap:code>KPI</cap:code>
```

The message comes into the system through an input queue. This queue is part of the messaging handling service.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Messaging handling
- Input queue name: IOC.CAP.IN
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```
- Logs:
 - /var/mqm/errors/AMQERR*.LOG
 - /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the input queue are an indication that the messaging services is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** command.

2. The messaging bus takes the message from the input queue and puts it in the output queue.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Messaging handling and message bus
- Output queue name: IOC_CAP_OUT
- Administration tools:
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)

- Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```

– Logs:

- /var/mqm/errors/AMQERR*.LOG
- /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the output queue are an indication that the CAP probe is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** command.

3. The CAP probe gets the message from the IOC_CAP_OUT queue and processes the message using rules. The probe uses a master rule that calls a CAP rules definition file. The XML CAP message is decomposed and put in to the correct tables in the Object Server NCOMS database. If the probe is able to successfully process the message, it is placed in the Object Server NCOMS database; otherwise, the message is discarded.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event handling
- Probe name: CAP
- Administration tools:
 - System Verification Check tool: Used to check the status of the event handling services. The Monitoring (Netcool/OMNIBus) test can be run to verify if this service is running.
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following commands can be used to query the status of the event handling services:

IBM Tivoli Netcool/OMNIBus process:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status ncob <password>
```

IBM Tivoli Netcool/OMNIBus probes:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status iocxml <password>
```

- Object Server NCOMS database configuration tool: Used to verify the NCOMS database status. The command is:

```
/opt/IBM/netcool/omnibus/bin/nco_config
```

– Logs:

- Probe log: /opt/IBM/netcool/omnibus/log/ioc_xml.log
- Object Server NCOMS database log: /opt/IBM/netcool/omnibus/log/NCOMS.log

Messages accumulating in the Object Server NCOMS database are an indication that the event reader is not able to process messages in timely manner. Verify if the event processing and enhancing services are running.

Important: If messages are not showing up in the Object Server NCOMS database, it might be because they are failing the CAP rule check that is performed by the probe. Make sure that the message is in the correct CAP format.

4. The object server informs the event reader, which picks up the message. The event reader is a service that runs in the event server. It processes the message according to the defined policies.

The main policy, IOC_Event_Main, invokes the other policies that process the message, decomposing it, and updating the IBM Intelligent Operations Center database. The IOC_Route_KPI_Event policy checks for the existence of the KPI code in the message and then updates the correct database tables. It also put the message in the IOC_KPI_IN queue.

- Service location: Event server
- Service name: Event processing and enhancing
- Event reader service name: IOC_CAP_Event_Reader

Event readers: Event readers are services that query events in data sources at some defined intervals and then apply defined policies to the event data.

- Message queue name: IOC_KPI_IN
- Policies names: IOC_Event_Main and IOC_Route_KPI_Event
- Administration tools:
 - System Verification Check tool: Used to check the status of the event processing and enhancing services. The Monitoring (Netcool/Impact Console) test can be run to verify if this service is running.
 - Platform Control tool (IOCControl): Used to verify and to start or stop selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status nci <password>
```
 - Administration Consoles: Event Processing and Enhancing (web-based console for Tivoli Netcool/Impact)
- Policies log: /opt/IBM/netcool/impact/log/NCI_policylogger.log

5. The event reader processes the message and the Tivoli Netcool/Impact server writes the decomposed message to the database, updating the IOC schema only.

Here are the various touch points for this step:

- Service location: Data server
- Service name: Database
- Database name: IOCDB
 - Database schemas name: IOC
 - Main database table name: IOC.CAPALERT
- Administration tools:
 - System Verification Check tool: Used to check the status of the database services. The following tests can be run to verify if this service is running:
Database (DB2 Instance - db2inst1)
Database (DB2)

- Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24sol <password>
```

- DB2 Control Center: db2cc as db2inst1 user

– Database log: /datahome/db2inst1/sqllib/log

6. The message bus takes the message from the IOC_KPI_IN input queue and puts it in the IOC_KPI_OUT output queue.

Here are the various touch points for this step:

– Service location: Event server

– Service name: Message bus

– Output queue name IOC_KPI_OUT

– Administration tools:

- WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
- System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:

Messaging (WebSphere Message Broker Publish/Subscribe topic)

Messaging (WebSphere Message Broker/Queue Install check)

Messaging (WebSphere Message Broker/Queue queue)

Messaging (WebSphere Message Queue Publish/Subscribe topic)

- Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```

– Logs:

- /var/mqm/errors/AMQERR*.LOG
- /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the output queue are an indication that the business monitoring is down. Run the System Verification Check tool to verify if the business monitoring services are running or restart the services with the **IOControl** command.

7. The business monitoring listens to the IOC_KPI_OUT queue. When a new KPI message appears in the queue, business monitoring takes it and processes it. KPI data is stored in the business monitoring database on the data server. If business monitoring identifies a status change in the KPI, it means that a notification flow must be initiated. A notification message is then put in the IOC_KPI_UPDATE queue.

Here are the various touch points for this step:

- Service location:
 - Application server
 - Data server
 - Event server
- Service names:
 - Business monitoring
 - Database
 - Messaging handling
- Database instance: db2inst4
- Database names: MONITOR and WBMDB
- Queue name: IOC_KPI_UPDATE
- Administration tools:
 - System Verification Check tool: Used to check the status of the messaging handling, database, and business monitoring services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Database (DB2 Instance - db2inst4)
 - Database (DB2)
 - Monitoring (WebSphere Business Monitor Business Space Console)
 - Monitoring (WebSphere Business Monitor Mobile Device Console)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following commands can be used to query the status of the messaging handling, database, and business monitoring services:
 - `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>`
 - `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24wmb <password>`
 - `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wbm <password>`
 - Administration consoles: Application Server (web-based console for WebSphere Application Server)
 - DB2 Control Center: db2cc as db2inst4 user
- Logs:
 - Business monitoring logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
 - Database logs: /datahome/db2inst4/sql1lib/log

8. The Message Driven Bean (MDB) portlet listens to the IOC_KPI_UPDATE queue. When a new notification message is available in the queue, it sends it to the KPI Manager portlet, which periodically publishes through the Publisher Services portlet and initiates the notification flow (see 7.4, “Notification flow” on page 206).

The KPI Manager also periodically updates the Key Performance Indicator Status and Key Performance Indicator Drill Down portlets. The time interval for the updates is configurable.

Here are the various touch points for this step:

- Service location: Application server
- Service name: Portal
- Portlets names:
 - Sample Event Publisher portlet
 - Key Performance Indicator Status portlet
 - Key Performance Indicator Drill Down portlet
- Administration tools:
 - Platform Control tool (**IOControl**): Used to verify and to start and stop selected services. The following commands can be used to query the status of the portal services:

```
opt/IBM/ISP/mgmt/scripts/IOControl.sh status wpe <password>
opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24po <password>
```
 - Administration consoles: Application Server (web-based console for WebSphere Application Server)
 - DB2 Control Center: db2cc as db2inst2 user
- Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

7.3 Correlation flow

The correlation flow applies predefined rules to search for a correlation among the incoming events. The purpose of this flow is to provide a mechanism to warn authorities, managers, or operators whenever there is a situation that demands their attention. The warning is triggered in the form of a notification that is sent whenever the inputs match the criteria that are defined in the rule.

The default rule analyses time and location. It triggers a notification whenever two events happen within 5 miles of one another and under 2 hours between them. It is supplied as an example, and most customers will customize the solution with their own correlation rules.

Figure 7-3 presents the correlation flow.

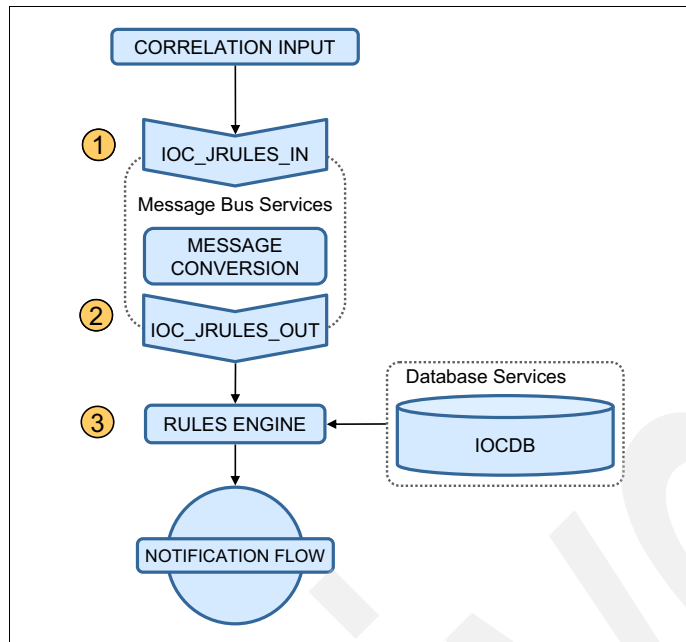


Figure 7-3 Correlation flow

The following steps correspond to the correlation flow steps shown in Figure 7-3:

1. The correlation flow starts when an event is sent to the IOC_JRULES_IN queue. This action is done by the IOC_Event_Correlation policy, in the event processing and enhancing service, as described in 7.1, “Event flow” on page 190.

The message comes into the flow through an input queue. This queue is part of the messaging handling service.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Messaging handling and message bus
- Input queue name: IOC_JRULES_IN
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```

- Logs:
 - /var/mqm/errors/AMQERR*.LOG.
 - /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG.

Important: Messages accumulating in the input queue are an indication that the messaging services is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** command.

2. The message bus takes the message from the input queue and transforms the message to convert it from text to the binary format required by the business rules engine. It then puts the binary message in the output queue.

Here are the various touch points for this step:

- Service location: Event server
- Service names: Messaging handling and message bus
- Output queue name: IOC_JRULES_OUT
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```
- Logs:
 - /var/mqm/errors/AMQERR*.LOG
 - /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the output queue are an indication that the business rules engine is down. Run the System Verification Check to verify if the services are running or restart the services with the **IOControl** command.

3. The business rules engine gets the message from the IOC_JRULES_OUT queue and processes the message using predefined correlation rules. It reads the database and verifies if the incoming event is correlated with events in the database. If a correlation is found, the business rules engine creates a notification message and initiates the notification flow (see 7.4, “Notification flow” on page 206).

Here are the various touch points for this step:

- Service location: Application server
- Service name: Business rules

- Administration tools:
 - System Verification Check tool: Used to check the status of the business rules services. The following tests can be run to verify if these services are running:
Business Rules (WebSphere Operational Decision Manager JRules Console)
Business Rules (WebSphere Operational Decision Manager JRules Rule)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following commands can be used to query the status of the business rules services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wdm <password>
```

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wdmc <password>
```
- Logs:
 - /opt/IBM/WebSphere/AppServer/profiles/wdmProfile1/logs/wdmServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/wdmProfile1/logs/wdmServer1/SystemErr.log

7.4 Notification flow

The notification flow handles a special XML message called *notification*. It processes this message and displays it in the notification portlet.

Notifications are warning messages that are triggered either by KPI status changes or events correlation. Their purpose is to allow authorities, managers, or operators to be aware of situations that might require their attention.

Figure 7-4 presents the notification flow.

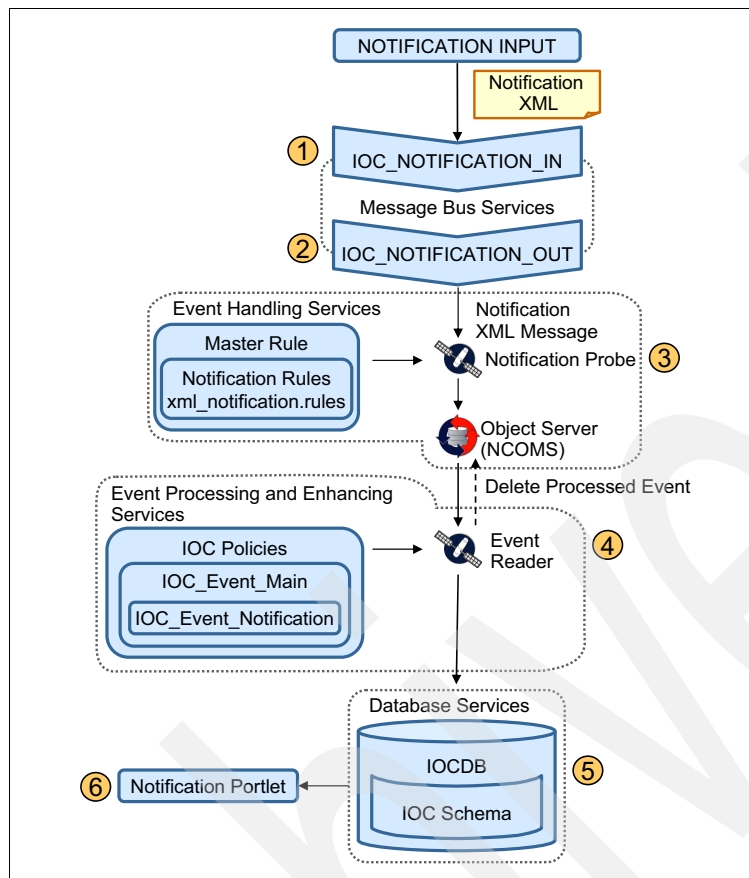


Figure 7-4 Notification flow

The following steps correspond to the notification flow steps shown in Figure 7-4:

1. The notification flow starts when a notification input is sent to the notification input queue, IOC_NOTIFICATION_IN. The sources for the notification can be the business monitoring services in the KPI flow or the business rules service in the correlation flow.

The message comes into the flow through an input queue. This queue is part of the messaging handling service.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Message bus
- Input queue name: IOC_NOTIFICATION_IN
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)

Messaging (WebSphere Message Broker/Queue queue)

Messaging (WebSphere Message Queue Publish/Subscribe topic)

- Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```

– Logs:

- /var/mqm/errors/AMQERR*.LOG
- /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the input queue are an indication that the messaging services is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** tool.

2. The message bus takes the message from the input queue and puts it in the output queue.

– Service location: Event server

– Service name: Message bus

– Output queue name: IOC_NOTIFICATION_OUT

– Administration tools:

- WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue
- System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:

Messaging (WebSphere Message Broker Publish/Subscribe topic)

Messaging (WebSphere Message Broker/Queue Install check)

Messaging (WebSphere Message Broker/Queue queue)

Messaging (WebSphere Message Queue Publish/Subscribe topic)

- Platform Control tool (**IOControl**): Used to verify and to start and stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```

– Logs:

- /var/mqm/errors/AMQERR*.LOG
- /var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.LOG

Important: Messages accumulating in the output queue are an indication that the Notification probe is down. Run the System Verification Check tool to verify if the messaging services are running or restart the services with the **IOControl** command.

3. The notification probe, which is part of the event handling services, gets the message from the IOC_NOTIFICATION_OUT queue and processes the message using rules. The probe uses a master rule that calls a notification rules definition file. The XML notification message is decomposed and put in to the correct tables in the Object Server NCOMS database. If the probe is able to successfully process the message, it is placed in the Object Server NCOMS database; otherwise, the message is discarded.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event handling
- Probe name: Notification
- Administration tools:
 - System Verification Check tool: Used to check the status of the event handling services. The following test can be run to verify if this service is running:
Monitoring (Netcool/OMNIBus)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following commands can be used to query the status of the event handling services:
IBM Tivoli Netcool/OMNIBus process:
`/opt/IBM/ISP/mgmt/scripts/IOControl.sh status ncob <password>`
IBM Tivoli Netcool/OMNIBus probes:
`/opt/IBM/ISP/mgmt/scripts/IOControl.sh status iocxml <password>`
 - Object Server NCOMS database configuration tool: Used to verify the NCOMS database status. Run the following command:
`/opt/IBM/netcool/omnibus/bin/nco_config`
- Logs:
 - Probe log: `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
 - Object Server NCOMS database log: `/opt/IBM/netcool/omnibus/log/NCOMS.log`

Important: Messages accumulating in the Object Server NCOMS database are an indication that the event reader is not able to process messages in timely manner. Verify if the event processing and enhancing services are running.

4. The Object Server NCOMS database informs the event reader, which picks up the message. The event reader is a service that runs in the event server. It processes the message by following the defined policies.

The main policy, called IOC_Event_Main, invokes the other policies that process the message, decomposing it and updating the IBM Intelligent Operations Center database. The IOC_Event_Notification policy validates the message and updates the correct database tables.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event processing and enhancing
- Event reader service name: IOC_Notification_Reader

Event readers: Event readers are services that query events in data sources at some defined intervals and then apply defined policies to the event data.

- Policies names: IOC_Event_Main and IOC_Event_Notification
 - Administration tools:
 - System Verification Check tool: Used to check the status of the Event processing and enhancing services. The Monitoring (Netcool/Impact Console) test can be run to verify if this service is running:
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status nci <password>
```
 - Administration consoles: Event Processing and Enhancing (web-based console for Tivoli Netcool/Impact)
 - Policies log: /opt/IBM/netcool/impact/log/NCI_policylogger.log
5. The event reader writes the decomposed message to the database, updating the IOC schema only.

Here are the various touch points for this step:

- Service location: Data server
 - Service name: Database
 - Database name: IOCDB
 - Database schemas names: IOC
 - Main database table names: IOC.NOTIFICATION
 - Administration tools:
 - System Verification Check tool: Used to check the status of the database services. The following tests can be run to verify if this service is running:
Database (DB2 Instance - db2inst1)
Database (DB2)
 - Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the event processing and enhancing services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24s01 <password>
```
 - DB2 Control Center: db2cc as db2inst1 user
 - Database logs: /datahome/db2inst1/sqllib/log
6. The event update servlet notifies the data provider that updates are available for users. Event data providers are the portlets responsible for the presentation of the user interface. The event data provider retrieves the latest data from the database and updates the user interface. The notification portlet is updated.

Here are the various touch points for this step:

- Service location: Application server
- Service name: Portal

- EAR names (applications that should be running in the application server)
 - ioc_portal_ear
 - iss_curi_ear
 - iss_help_war
 - iss_portal_ear
- Portlets name: Notifications portlet
- Administration tools:
 - Platform Control tool (**IOControl**): Used to verify and start or stop selected services. The following commands can be used to query the status of the portal services:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wpe <password>
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24po <password>
```
 - Administration consoles: Application Server (web-based console for WebSphere Application Server)
 - DB2 Control Center: db2cc as db2inst1 user
- Logs:
 - Portal logs:


```
/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
```
 - Database log: /datahome/db2inst1/sqllib/log

7.5 Resource flow

Resources in IBM Intelligent Operations Center are specialized assets with location and capabilities information, such as hospitals or warehouses. Resources have the following attributes:

- ▶ Unique ID
- ▶ Description
- ▶ Calendar
- ▶ Shift
- ▶ Operating site
- ▶ Status
- ▶ Priority of operation
- ▶ Service address
- ▶ Billing address
- ▶ Shipping address
- ▶ Address
- ▶ Geospatial coordinates (longitude and latitude positions)

Figure 7-5 shows a sample hospital resource.

The screenshot shows the 'Resources (IntOpCtr)' application interface. The 'Resource' tab is active, displaying details for 'Bascom Eye Institute' (Resource ID: BASCOMMEYE). The 'Short Description' is 'Recognized international leaders in macular, retinal and optic nerve diseases, cataracts, eye infections, eye cancers and eye diseases in children'. The 'Site' is 'PMSCRTP'. Below this is a 'Localization' section with fields for 'Street Address' (900 N.W. 17th Street), 'City' (Miami), 'State' (FL), 'Address Line 2', and 'Country' (USA). There are also fields for 'Calendar' and 'Shift'.

Figure 7-5 Sample resource

Capabilities (which are located under the Capabilities tab) are specialized classifications with attributes. For example, ER, burn unit, and pediatric are capabilities for a hospital classified resource. Capabilities are associated with a resource to provide the quality of service.

Figure 7-6 shows an example for Bascom Eye Institute, which is a classified hospital resource with a burn unit, ER, heliport, and pediatric as capabilities.

The screenshot shows the 'Resources (IntOpCtr)' application interface with the 'Capabilities' tab active. The resource is 'Bascom Eye Institute' (Resource ID: BASCOMMEYE). The 'Classification' is 'RESOURCE \ HOSPITAL' and the 'Class Description' is 'RESOURCES \ HOSPITAL'. Below this is a table of capabilities:

Attribute	Description	Numeric Value	Unit of Measure
BURNUNIT	The capacity of the burn unit in the hospital.		
ER	The capacity of the emergency room in the hospital.	1.0	
HELIPORT	The capacity of the heliport in the hospital.		
PEDIATRIC	The capacity of the pediatric room in the hospital.		
TRAUMACENTER	The capacity of the trauma center in the hospital.		

Below the table is a 'Details' section for the selected 'BURNUNIT' capability, showing the attribute name, description, and a numeric value field.

Figure 7-6 Sample capabilities

Resources and capabilities are initially created and stored in the event server under the IBM Tivoli Service Request Manager application. IBM Intelligent Operations Center polls the capabilities and stores them in the IOCD database IOC.CAPABILITY table. IBM Intelligent Operations Center also maps these capabilities to CAP message-based categories, as defined in the IBM Intelligent Operations Center.

Resources are listed in the IBM Intelligent Operations Center with authorized access to Supervisor:Operations or Operator:Operations page in the Details portlet. On the Event and Incidents tab, right-click any event and select **View Nearby Resources**. The list of associated resources is displayed in the Resource tab in the Details portlet.

As an authorized user, you can view, update, or delete the resources that are listed in the Resource tab. Each of these operations results in a resource message flow (Figure 7-7).

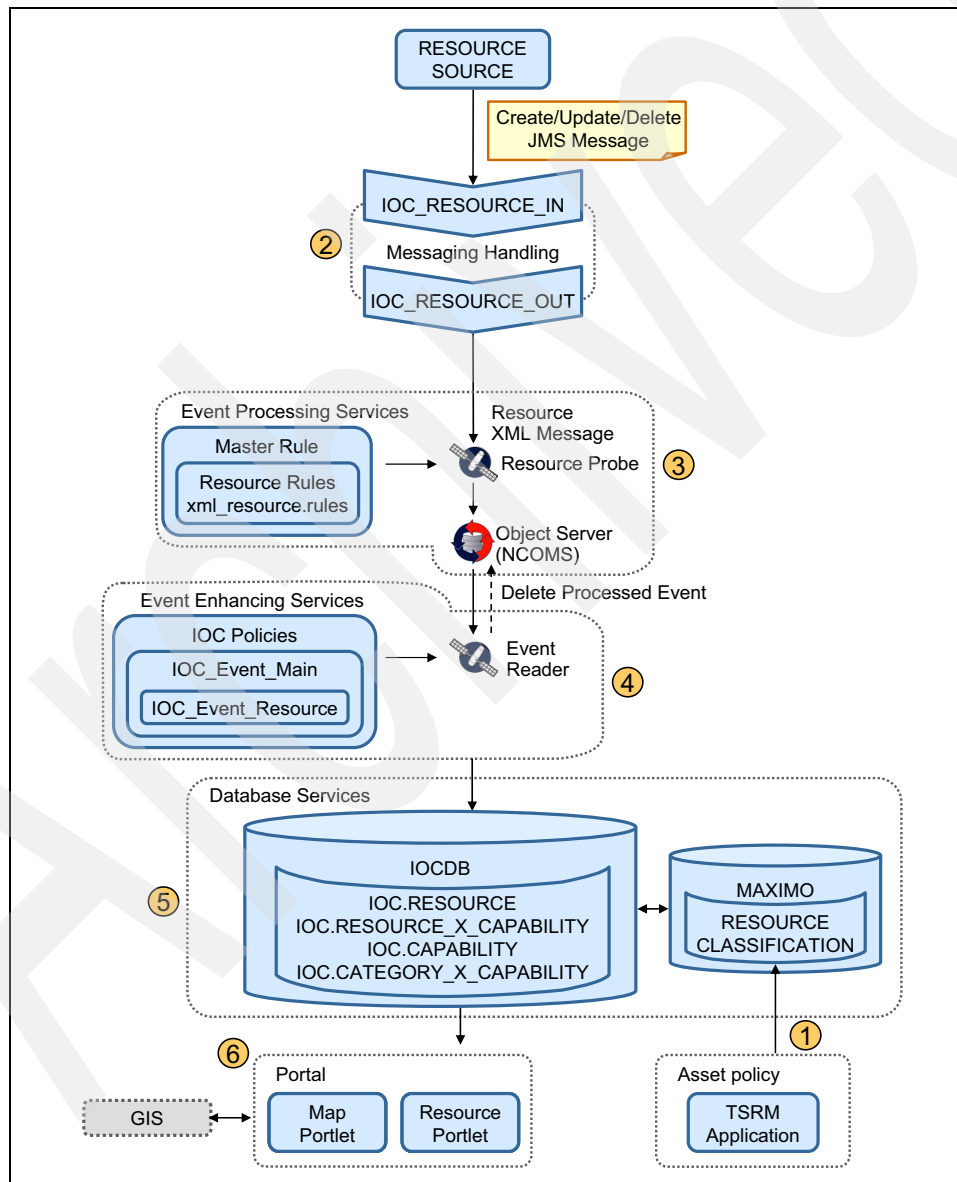


Figure 7-7 Resource data flow

Resources are stored in an IBM Tivoli Service Request Manager database that is called MAXIMO in the RESOURCE table. The capabilities are stored in the CLASSIFICATION table. Key elements of these resources and capabilities, such as ID, name, location, contact, and capabilities, are transferred to IBM Intelligent Operations Center IOCDDB database through an internal solution integration framework.

In the IOCDDB database, resources and capabilities are stored with following information and mapping:

- ▶ IOC.RESOURCE: Key resource information
- ▶ IOC.RESOURCE_X_CAPABILITY: Number of resources that are mapped to capabilities
- ▶ IOC.CAPABILITY: Key capability information
- ▶ IOC.CATEGORY_X_CAPABILITY: Capabilities that are mapped to event categories

The following steps correspond to the resource data flow steps shown in Figure 7-7 on page 213:

1. Initially, an authorized user creates the resources and capabilities in IBM Tivoli Service Request Manager console.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Resource management (IBM Tivoli Service Request Manager)
- Database name: MAXIMO
- Database schemas name: MAXIMO
- Main database table names: MAXIMO.RESOURCE and MAXIMO.CLASSIFICATION
- Administration tools:
 - System Verification Check tool: Used to check the status of the database and standard operating procedure administration services. The following tests can be run to verify if this service is running:
 - Database (DB2 Instance - db2inst6)
 - Database (DB2)
 - Policy (Tivoli Service Request Manager Maximo Console)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following commands can be used to query the status of the database and standard operating procedure administration services:
 - `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24tsrm <password>`
 - `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status tsrm <password>`
 - DB2 Control Center: db2cc as db2inst6 user.
- Logs:
 - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log`

2. When a resource is created, updated, or deleted, the underlying IBM Tivoli Service Request Manager creates a resource message and sends it to the IOC_RESOURCE_IN message queue in the message bus. The message bus internally processes the incoming JMS-based resource message, converts it to an XML format, and passes it to the IOC_RESOURCE_OUT queue.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Messaging handling
- Input queue name: IOC_RESOURCE_IN
- Output queue name: IOC_RESOURCE_OUT
- Administration tools:
 - WebSphere MQ Explorer: Used to verify if messages are accumulating in the queue.
 - System Verification Check tool: Used to check the status of the messaging handling and message bus services. The following tests can be run to verify if these services are running:
 - Messaging (WebSphere Message Broker Publish/Subscribe topic)
 - Messaging (WebSphere Message Broker/Queue Install check)
 - Messaging (WebSphere Message Broker/Queue queue)
 - Messaging (WebSphere Message Queue Publish/Subscribe topic)
 - Platform Control tool (**IOControl**): Used to verify and to start or stop selected services. The following command can be used to query the status of the messaging handling and message bus services:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wmb <password>
```
- Logs:
 - /var/logs/errors
 - /var/mqm/qmgrs/IOC!MB!QM/errors

3. The resource probe receives the message from the IOC_RESOURCE_OUT queue and processes the message using rules. The probe uses a master rule that calls a resource rule definition file. The resource XML message is stored in the Object Server NCOMS database. The message is then handed to the event processing and enhancing service.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event handling
- Probe name: Resource
- Administration tools:
 - System Verification Check tool: Used to check the status of the event handling services. The Monitoring (Netcool/OMNIBus) test can be run to verify if this service is running.
 - Platform Control tool (**IOControl**): Used to verify and manage selected services. The following commands can be used to query the status of the event handling services:
 - IBM Tivoli Netcool/OMNIBus process:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status ncob <password>
```
 - IBM Tivoli Netcool/OMNIBus probes:

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status iocxml <password>
```

- Object Server NCOMS database configuration tool: Used to verify the NCOMS database status:

`/opt/IBM/netcool/omnibus/bin/nco_config`

– Logs:

- Probe log: `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- Object Server NCOMS database log: `/opt/IBM/netcool/omnibus/log/NCOMS.log`

4. The event reader reads the message when handed over by the probe. The event reader is part of event processing and enhancing service that runs in the event server. It processes the message by following the defined policies. The `IOC_Event_Resource` policy validates and processes the message before it updates the database tables.

Here are the various touch points for this step:

- Service location: Event server
- Service name: Event processing and enhancing
- Event reader service name: `IOC_Resource_Event_Reader`

Event readers: Event readers are services that query events in data sources at some defined intervals and then apply defined policies to the event data.

– Policies names: `IOC_Event_Resource`

– Administration tools:

- System Verification Check tool: Used to check the status of the event processing and enhancing services. The Monitoring (Netcool/Impact Console) test can be run to verify if this service is running.
- Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the event processing and enhancing services:

`/opt/IBM/ISP/mgmt/scripts/IOControl.sh status nci <password>`

- Administration consoles: Event Processing and Enhancing (web-based console for Tivoli Netcool/Impact)

– Log: `/opt/IBM/netcool/impact/log`

5. After the event processing and enhancing processes the message, it is decomposed and stored in IBM Intelligent Operations Center database tables. The capabilities are polled by IBM Intelligent Operations Center through integration at regular intervals and stored in the database tables.

Here are the various touch points for this step:

- Service location: Data server
- Service name: Database
- Database name: `IOCDB`
- Database schemas names: `IOC`
- Main database table names:
 - `IOC.RESOURCE`
 - `IOC.RESOURCE_X_CAPABILITY`
 - `IOC.CAPABILITY`
 - `IOC.CATEGORY_X_CAPABILITY`

- Administration tools:
 - System Verification Check tool: Used to check the status of the database services. The following tests can be run to verify if this service is running:
 - Database (DB2 Instance - db2inst1)
 - Database (DB2)
 - Platform Control tool (**IOControl**): Used to verify and manage selected services. The following command can be used to query the status of the event processing and enhancing services:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status db24so1 <password>
```
 - DB2 Control Center: db2cc as db2inst1 user.
 - Database logs:
 - /home/db2inst1/sqllib/log/db2start*.log
 - /home/db2inst1/sqllib/log/instance.log
6. On successful processing of the message in the database, the event update servlet notifies the data provider that updates are available for users. Event data providers are the portlets responsible for the presentation of the user interface. The event data provider retrieves the latest data from the database and updates the user interface. The updated resources can be seen on the portal by completing the following steps:
- a. Go to the Supervisor:Operations page, click the **Details** portlet, and click the **Event and Incidents** tab.
 - b. Right-click an event row and select **View Nearby Resources → 100 miles** (or a preferred mile range from the list).
 - c. The updated resources are displayed in the Details portlet Resource tab.
 - d. Right-click a resource row and select Properties to view the updated changes or make any changes.

Updates in Resource portlet: Any updates that are made to a resource in the Resource portlet forces a resource message to be generated and the resource flow to begin.

Here are the various touch points for this step:

- Service location: Application server
- Service name: Portal
- EAR names (applications that should be running in the application server):
 - ioc_portal_ear
 - iss_curi_ear
 - iss_help_war
 - iss_portal_ear
- Portlets names:
 - Details portlet (under the Resource tab)
 - Map portlet
- Administration tools:
 - Platform Control tool (**IOControl**). Use the following command to query the status of the portal services:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status wpe <password>
```

- Administration consoles: Application Server (web-based console for WebSphere Application Server)
- Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

7.6 User authentication and authorization flow

The user authentication and authorization flow describes how the user authentication and authorization process grants access to the resources within the IBM Intelligent Operations Center.

Figure 7-8 presents an overview of the user authentication and authorization flow.

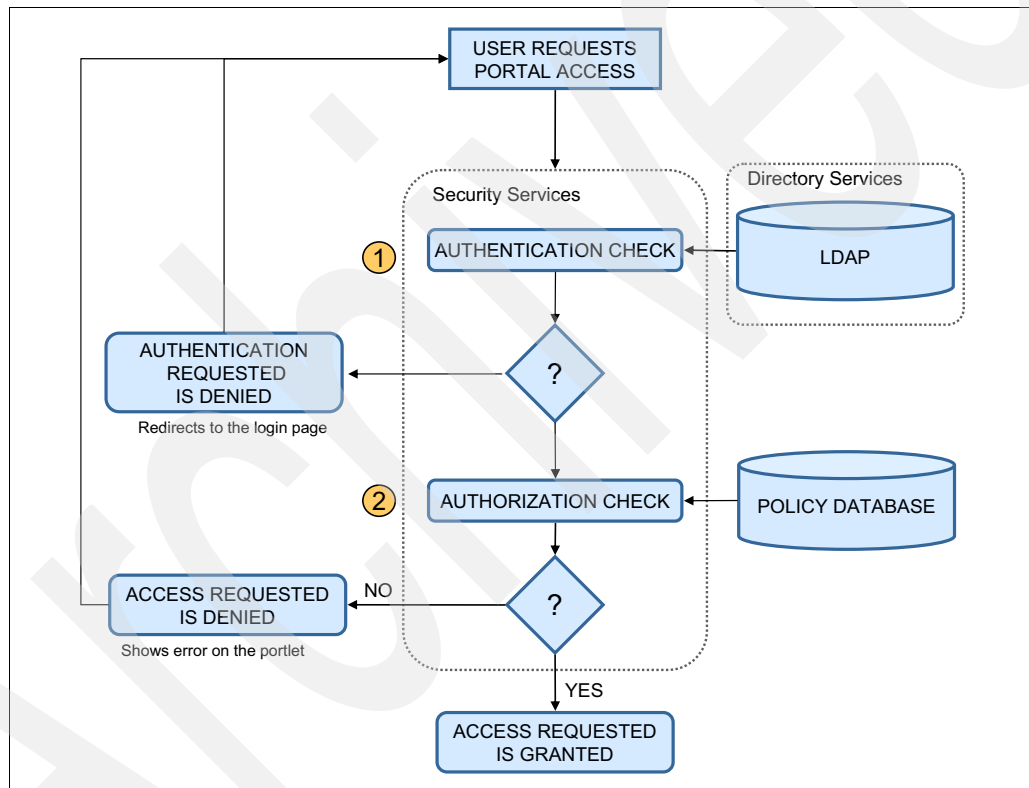


Figure 7-8 User authentication and authorization flow

The following steps correspond to the user authentication and authorization flow steps that are shown in Figure 7-8:

1. The user authentication and authorization flow starts when a user requests a login to the IBM Intelligent Operations Center. The user opens the portal login page and enters a user ID and password. The security service performs an authentication check by verifying the user credentials against the LDAP directory. If the credentials do not match the ones in the LDAP directory, the requested access is denied and the user is redirected to the login page. If the credentials match, the flow continues to the next step.

Here are the various touch points for this step:

- Service location: Management server
- Service name: Security service
- Administration tools:
 - Portal Access (under Users and Groups)
 - Directory (web-based console for Tivoli Directory Server)
- Logs:
 - /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log
 - /datahome/dsrdbm01 /idsslapd- dsrdbm01/logs/ directory

2. After the authentication of the user, an authorization check is performed by verifying the policy database. This check indicates if the user has authorized access to the requested resource. If the user is not authorized, an error message is displayed in the portlet; otherwise, access to the resource is granted.

Here are the various touch points for this step:

- Service location: Management server
- Service name: Security
- Administration tools:
 - Portal Access (under Resource Permissions)
 - Application Server for Management (web-based console for WebSphere Application Server for Management, including Tivoli Access Manager and WebSEAL)
- Logs:
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log

7.7 Overall system flows

This section combines all the message flows described in this chapter and provides a global picture of the IBM Intelligent Operations Center data flow architecture. Figure 7-9 provides the core data flow diagram that shows the interaction of external and internal subsystems. The messages are read, transformed, or analyzed against system or business rules as they pass through the subsystems.

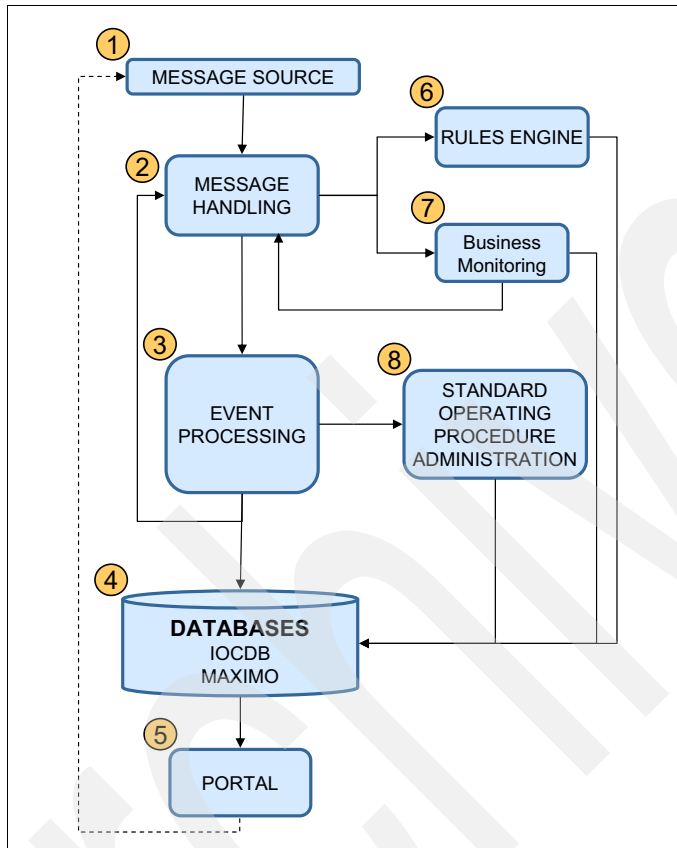


Figure 7-9 IBM Intelligent Operations Center system flow overview

The messages flow through the various IBM Intelligent Operations Center and external systems using the following basic steps:

1. The message is generated from a source. This source can be an external system or IBM Intelligent Operations Center internal tool. The messages are of various kinds, such as Common Access protocol (CAP) based events, KPIs, notifications, or resources. The flow starts when a message or event is sent to the IBM Intelligent Operations Center.

Non-CAP messages: A non-CAP message that is required to be transformed to CAP message or special handling or non-CAP data is out of the scope of this book, because it requires customization.

2. Messages from the data sources are processed through the message queues in the message bus services. The message bus has at least one input queue and its corresponding output queue to hand over the message for further processing.

3. In general, the messages move from the message bus output queue to the event processing service. The event processing service consists of event handling and event processing and enhancing services. The messages are checked for appropriate formatting by the event handling service before they pass to the event processing and enhancing. Various system rules are checked at this level.
4. Most of the messages are decomposed and written to the IBM Intelligent Operations Center database.
5. Messages that are written to the IBM Intelligent Operations Center database are read and displayed by the portal service in the appropriate portlet. Event data flow is one simple example of such a flow.
6. Messages that require validation, such as correlation rules or other business rules, are passed to the rules engine through the event processing service through the rule-based message queues before they are written to the database. After the evaluation by the rules engine, the messages are written to the database.
7. The event processing service also recognizes KPI messages and sends them to KPI queues before it hands them over to the business monitoring service. The business monitoring service evaluates against the ranges and publishes notification messages through queues before it writes them to the database.
8. Event processing services hands over the incoming events to verify if its elements have a matching SOP matrix. If the match is found, the corresponding SOP creates the specified activities and tasks. The SOP activities appear on My Activities portlet for the assigned users.

Archived

Related publications

The publications that are listed in this section are considered suitable for a more detailed discussion of the topics that are covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Some publications referenced in this list might be available in softcopy only.

- ▶ *Certification Guide Series: IBM Tivoli Netcool/Impact V4.0 Implementation*, SG24-7755
- ▶ *Certification Guide Series: IBM Tivoli Netcool/OMNIBus V7.2 Implementation*, SG24-7753
- ▶ *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443

You can search for, view, download, or order these documents and other Redbooks, Redpapers, Web Docs, drafts, and more materials at the following website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- ▶ *IBM Intelligent Operations Center 1.5 Passwords Management Document*:
<http://www.ibm.com/support/docview.wss?uid=swg2161122>
- ▶ *IBM Tivoli Access Manager for e-business Troubleshooting Guide*:
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am611_problem.htm
- ▶ *IBM Tivoli Directory Server Version 6.3 Command Reference*:
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/command_ref.pdf
- ▶ “Tivoli Directory Server 6.1 password policy: enhancements, configuration, and troubleshooting”:
<http://www.ibm.com/developerworks/tivoli/library/t-tdspp-ect/>
- ▶ *Tivoli Enterprise Portal User's Guide*:
http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itm.doc_6.2.2fp2/itm622fp2_tepuser.htm
- ▶ WebSphere Portal 8 product documentation:
<http://www-10.lotus.com/ldd/portalwiki.nsf/xpViewCategories.xsp?lookupName=IBM%20WebSphere%20Portal%20%20Product%20Documentation>

Online resources

These websites are also relevant as further information sources:

- ▶ Common Alerting Protocol (CAP) format:
<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- ▶ IBM DB2 Universal Database Information Center:
<http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp>
- ▶ IBM Intelligent Operations Center Product page:
<http://www-01.ibm.com/software/industry/intelligent-oper-center/>
- ▶ IBM Intelligent Operations Center V1.5 announcement letter:
<http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS212-250&apname=USN>
- ▶ IBM Intelligent Operations Center V1.5 Information Center:
<http://pic.dhe.ibm.com/infocenter/cities/v1r5m0/topic/com.ibm.ioc.doc/ic-homepage.html>
- ▶ IBM Smarter City Solution on Cloud:
<http://www-01.ibm.com/software/industry/smartercities-on-cloud/>
- ▶ IBM Tivoli Access Manager for e-business Version 6.1.1 Information Center
<http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/welcome.htm>
- ▶ IBM Tivoli Directory Server Information Center:
<http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm>
- ▶ IBM Tivoli Monitoring Information Center:
http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.1/welcome.htm
- ▶ Oasis open standards:
<https://www.oasis-open.org/standards#uddiv3.0.2>
- ▶ Solutions for Smarter Cities application store:
https://www-304.ibm.com/sales/gss/download/industry_solutions_catalog/CrossIndustrySolutions.do?industry=cities

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



IBM Intelligent Operations Center for Smarter Cities Administration Guide

(0.2" spine)
0.17" x 0.473"
90 x 249 pages



IBM Intelligent Operations Center for Smarter Cities Administration Guide



All you need to know to administer IBM Intelligent Operations Center

Tools, tips, and techniques for administrators

Troubleshooting scenarios for administrators

IBM defines a smarter city as one that makes optimal use of all available information to better understand and control its operations and optimize the use of resources. There is much information available from different sources. However, city officials often lack the holistic view of the city's operations that is required to respond to the citizens' needs in a timely manner and use the city resources wisely.

IBM Intelligent Operations Center delivers a unified view of city agencies, providing three primary elements for successful management of cities:

- ▶ Use information.
- ▶ Anticipate problems.
- ▶ Coordinate actions and resources.

Chapter 1 of this IBM Redbooks publication introduces the IBM Intelligent Operations Center solution. The chapter provides a high-level overview of its features, benefits, and architecture. This information is intended for city officials and IT architects that must understand the business value of IBM Intelligent Operations Center and its architecture.

The remaining chapters of this book focus on information that help IBM Intelligent Operations Center administrators perform daily administration tasks. This book describes commands and tools that IBM Intelligent Operations Center administrators must use to keep the solution running, troubleshoot and diagnose problems, and perform preventive maintenance. This book includes preferred practices, tips and techniques, and general suggestions for administrators of IBM Intelligent Operations Center on-premises deployments.

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

SG24-8061-00

ISBN 0738437492