

IBM Intelligent Operations Center
Version 1 Release 5

*IBM Intelligent Operations Center
Product Documentation*



IBM Intelligent Operations Center
Version 1 Release 5

*IBM Intelligent Operations Center
Product Documentation*



Note

Before using this information and the product it supports, read the information in "Notices" on page 341.

This edition applies to IBM Intelligent Operations Center version 1, release 5, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2011, 2012.**

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

Contents

| | |
|--------------------------|-----------|
| Figures | ix |
|--------------------------|-----------|

| | |
|--|----------|
| Chapter 1. Solution overview. | 1 |
|--|----------|

| | |
|--|---|
| Intended audience | 1 |
| Features | 2 |
| Users and benefits | 3 |
| Components | 5 |
| Event management | 7 |
| What's new in version 1.5 | 8 |
| What's new for the user | 8 |
| What's new for the administrator | 9 |

| | |
|--|-----------|
| Chapter 2. Installing and configuring | 11 |
|--|-----------|

| | |
|---|----|
| Preparing for installation | 11 |
| IBM Intelligent Operations Center system services | 11 |
| IBM Intelligent Operations Center hardware requirements | 12 |
| Prerequisite software requirements | 13 |
| Supported browsers | 13 |
| Media packaging | 14 |
| Installation checklists | 14 |
| Checklist - installing using IBM Installation Manager | 14 |
| Checklist - installing step-by-step | 15 |
| Preparing the servers | 17 |
| TCP/IP networking | 20 |
| Copying the installation package to the installation server | 23 |
| Installing the Java runtime environment | 24 |
| Installing IBM Intelligent Operations Center using Installation Manager | 25 |
| Installation components | 28 |
| Configuration options | 29 |
| Topology password | 29 |
| Installation media location | 29 |
| Data server location | 30 |
| Application server location | 30 |
| Event server location | 30 |
| Management server location | 31 |
| Cyber hygiene configuration | 31 |
| Restarting the installation using Installation Manager | 32 |
| Installing IBM Intelligent Operations Center step-by-step | 32 |
| Preparing the installation package | 32 |
| Verifying the installation scripts | 33 |
| Customizing the installation properties | 33 |
| Installation topology files | 34 |
| Topology properties file | 35 |
| Target server information | 35 |
| Directory services information | 36 |
| Password information | 36 |
| Creating the topology password | 39 |
| Generating the topology file | 39 |

| | |
|---|----|
| Running the Precheck tool | 40 |
| Linux security settings | 41 |
| Manually tailoring Linux security settings | 41 |
| Tailoring Linux security settings with a script | 41 |
| The installTopology command | 42 |
| Options for installing IBM Intelligent Operations Center components | 42 |
| Installing IBM Intelligent Operations Center architecture in a single phase | 43 |
| Installing IBM Intelligent Operations Center architecture in multiple phases | 44 |
| Restarting the IBM Intelligent Operations Center architecture installation during a step-by-step installation | 46 |
| Installing the Platform Control Tool | 46 |
| Installing the System Verification Check tool | 47 |
| Installing the IBM Intelligent Operations Center application | 48 |
| Verifying the installation | 48 |
| Post-installation IBM Intelligent Operations Center configuration | 49 |
| Configuring collaboration services for IPv6 | 49 |
| Configuring single sign-on for collaboration services | 50 |
| Setting the session timeout | 51 |
| Installing and configuring semantic model services | 52 |
| Configuring the Jazz team server | 52 |
| Installing semantic model services | 53 |
| Verifying semantic model services configuration | 54 |
| Improving semantic model services performance | 55 |
| Configuring the Platform Control Tool | 56 |
| Encrypting the Tivoli Service Request Manager administrative password | 56 |
| Setting the minimum number of threads for the EventProcessor | 57 |
| Changing the Default and WebContainer thread pool size | 57 |
| Installing and running cyber hygiene step-by-step | 58 |
| Changes to the Linux operating system | 60 |
| Reviewing the cyber hygiene log | 60 |
| Re-enabling remote root log on | 61 |
| Configuring users requiring ssh access | 62 |
| Installing tools provided with the solution | 62 |
| Deleting sample users | 63 |
| Removing installation services from the production system | 64 |

| | |
|---|-----------|
| Chapter 3. Securing the solution | 65 |
|---|-----------|

| | |
|--|----|
| User roles and access | 66 |
| Sample users | 67 |
| User role groups and authorization permissions | 68 |
| User category groups and data permissions | 70 |

| | |
|---|----|
| Adding a user or group | 71 |
| Viewing or modifying group membership | 72 |
| Viewing or editing a user profile | 73 |
| Deleting a user or group | 74 |
| Importing users and groups | 74 |
| User Permissions Summary | 76 |
| Cyber hygiene overview | 76 |
| Cyber security | 78 |
| Cyber hygiene checklists | 78 |
| Checklist item analysis | 78 |
| Checklist selection | 79 |
| Cyber hygiene default configuration | 80 |
| Default password management policies | 80 |
| Disabled Linux services | 81 |
| Removed user IDs | 82 |
| Audit rules | 83 |
| File and directory permissions | 83 |
| Other changes | 83 |
| Remediation tools | 84 |
| Cyber hygiene documentation | 85 |

Chapter 4. Integrating the solution 87

| | |
|--|-----|
| Examples of systems that can be integrated. | 87 |
| Integration points and protocols | 87 |
| Events and KPIs. | 87 |
| Policy for KPI updates. | 88 |
| Integrating with the Common Alerting Protocol | 89 |
| CAP structure | 90 |
| Event types | 91 |
| Using CAP for KPI events | 92 |
| Using CAP for non-KPI events | 95 |
| Using the inbound event queue defined for the IBM Intelligent Operations Center | 95 |
| Creating events using the Publisher service. | 96 |
| Developing with the common utility classes | 96 |
| Using the Publisher service | 97 |
| Using the Publisher servlet | 97 |
| Creating and publishing test events | 98 |
| Sample Publisher | 99 |
| Creating sample events with XML | 100 |
| Creating new CAP events or updating existing events without XML | 101 |
| Testing notifications | 102 |
| Event Scripting. | 103 |
| Viewing sample events and KPI events in the sample events table | 103 |
| Creating an event script | 104 |
| Creating and integrating KPIs | 105 |
| Monitor models and KPIs | 106 |
| Monitoring context instances | 107 |
| Modeling KPIs | 107 |
| Defining KPI hierarchies. | 110 |
| Defining KPI hierarchies with OWL | 111 |
| KPI event communication between IBM WebSphere Business Monitor and IBM Intelligent Operations Center | 112 |
| Triggers | 112 |
| Defining inbound events to IBM WebSphere Business Monitor | 113 |
| Defining outbound events to the IBM Intelligent Operations Center | 113 |

| | |
|--|-----|
| Deploying monitor models | 115 |
| KPI display values. | 115 |
| Caching KPIs | 116 |
| Sample KPIs. | 117 |
| Configuring Tivoli Service Request Manager | 119 |
| Using the Tivoli Service Request Manager user interface | 119 |
| Opening Tivoli Service Request Manager applications | 119 |
| Setting up favorite applications in the Tivoli Service Request Manager Start Center | 120 |
| Configuring new users in Tivoli Service Request Manager | 121 |
| Setting the Default Insert Site | 121 |
| Assigning a user to a security group | 121 |
| Assigning a user to a person group | 122 |
| Standard Operating Procedures | 123 |
| Creating workflows | 124 |
| Creating standard operating procedures | 124 |
| Reviewing entries in the standard operating procedure selection matrix | 126 |
| Defining parameters in the standard operating procedure selection matrix | 126 |
| Managing resources | 127 |
| Synchronizing the sample resources to the IBM Intelligent Operations Center database | 128 |
| Creating or modifying the event category to capability mapping | 128 |
| Creating a resource | 130 |
| Viewing, updating, or deleting a resource | 131 |
| Creating a resource type. | 132 |
| Adding a capability to a resource type | 132 |
| Sample standard operating procedures, workflows, and resources | 133 |

Chapter 5. Customizing the solution 135

| | |
|---|-----|
| Customizing the user interface | 135 |
| Localizing the user interface | 135 |
| List of portlets | 135 |
| User portlets | 135 |
| Administrative portlets | 137 |
| Creating or customizing a page | 138 |
| Customizing the portlets | 139 |
| About portlet settings | 139 |
| Administration Consoles portlet settings | 140 |
| Contacts portlet settings. | 140 |
| Details portlet settings | 141 |
| Key Performance Indicator Drill Down portlet settings | 145 |
| Key Performance Indicators portlet settings | 147 |
| Location Map portlet settings | 148 |
| Location Map Manager portlet settings. | 149 |
| Map portlet settings | 150 |
| My Activities portlet settings | 152 |
| Notifications portlet settings | 153 |
| Reports portlet settings | 154 |
| Sample Publisher portlet settings. | 155 |
| Standard Operating Procedures portlet settings | 156 |
| Status portlet settings. | 156 |
| Customizing the portlet help | 158 |

| | | | |
|--|------------|--|-----|
| Portlet help file locations | 158 | Required stop order | 189 |
| Customizing KPIs | 159 | Querying the status of the services | 191 |
| Key Performance Indicators | 160 | Getting help for the Platform Control Tool | 192 |
| Viewing KPI hierarchies | 160 | Administration Consoles | 192 |
| Changing a KPI hierarchy | 161 | Managing the services | 195 |
| Adding an owning organization | 161 | Application server | 195 |
| Changing the KPI legend | 162 | Data server | 196 |
| Viewing a KPI model | 162 | Event server | 196 |
| Viewing or changing a KPI | 162 | Management server | 198 |
| Copying a KPI | 163 | Verifying the components | 199 |
| Creating a KPI | 163 | How to use the System Verification Check tool | 199 |
| Sample KPIs | 163 | System Verification Check tests | 200 |
| Customizing the Key Performance Indicators portlet | 163 | Account Management (Tivoli Identity Manager API) Test | 200 |
| Back up before customizing KPIs | 164 | Problem determination | 200 |
| Customizing event correlation | 165 | Account Management (Tivoli Identity Manager Console) Test | 202 |
| Event correlation and the rules application | 165 | Problem determination | 202 |
| Customizing event correlation settings | 165 | Account Management (Tivoli Directory Integrator list assembly) Test | 204 |
| Modifying decision properties | 166 | Problem determination | 204 |
| Editing the decision table | 166 | Account Management (Tivoli Directory Server) Test | 206 |
| Changing decision table properties | 167 | Problem determination | 206 |
| Deploying the modified rule set to the IBM Intelligent Operations Center flow | 167 | Analytics (Cognos Gateway Console) Test | 207 |
| Location Map Manager | 168 | Problem determination | 207 |
| Adding a classification to the map menu | 168 | Application Server (WebSphere Application Server Web Service) Test | 209 |
| Adding a map to the portlet | 168 | Problem determination | 209 |
| Adding or changing areas on a location map | 169 | Business Rules (WebSphere Operational Decision Manager JRules Console) Test | 211 |
| Customizing the Location Map Manager portlet | 169 | Problem determination | 211 |
| Specifying system-wide configuration data | 170 | Business Rules (WebSphere Operational Decision Manager JRules Rule) Test | 213 |
| Updating the system properties table | 174 | Problem determination | 213 |
| Configuring IBM Cognos Business Intelligence to create reports | 175 | Collaboration (Lotus Domino console) Test | 215 |
| Creating a Reports portlet | 175 | Problem determination | 215 |
| Editing the Reports portlet layout | 175 | Collaboration (Lotus Sametime console) Test | 216 |
| Customizing a portlet to display reports | 176 | Problem determination | 216 |
| Locating the report URL | 177 | Collaboration (Lotus Sametime Proxy console) Test | 217 |
| Working with the data model | 177 | Problem determination | 217 |
| Generating the common schema data model reports | 177 | Database (DB2) Test | 219 |
| Pie chart options | 178 | Problem determination | 219 |
| Table chart options | 178 | Database (DB2 Instance - <i>instance</i>) Test | 220 |
| Generating the Common Alerting Protocol schema data model reports | 179 | Problem determination | 220 |
| Data model report options | 179 | Directory (UDDI V3 and UDDI V3 HTTPS) Test | 221 |
| Pie chart options | 180 | Problem determination | 221 |
| User-defined events reports options | 181 | Internal Diagnostic (Echo REST remoted) Test | 223 |
| User-defined custom report options | 182 | Problem determination | 223 |
| Configuring common schema data model reports | 182 | Messaging (WebSphere Message Broker Publish/Subscribe topic) Test | 225 |
| Configuring Common Alerting Protocol schema data model reports | 183 | Problem determination | 225 |
| More reports options | 183 | Messaging (WebSphere Message Queue Publish/Subscribe topic) Test | 226 |
| | | Problem determination | 226 |
| | | Messaging (Message Broker install check) Test | 227 |
| | | Problem determination | 227 |
| Chapter 6. Managing the solution. | 185 | | |
| About | 185 | | |
| Controlling the services | 185 | | |
| Starting the services | 185 | | |
| Required start order | 186 | | |
| Starting and stopping the Tivoli Netcool/OMNIbus probe | 188 | | |
| Stopping the services | 188 | | |

| | |
|--|-----|
| Messaging (WebSphere Message Broker/Queue queue) Test | 228 |
| Problem determination | 228 |
| Monitoring (Netcool Impact Console) Test | 229 |
| Problem determination | 229 |
| Monitoring (Netcool Omnibus) Test | 229 |
| Problem determination | 230 |
| Monitoring (Tivoli Composite Application Manager Agents - <i>server</i>) Test | 230 |
| Problem determination | 231 |
| Monitoring (Tivoli Enterprise Monitoring Server) Test | 231 |
| Problem determination | 232 |
| Monitoring (WebSphere Business Monitor Business Space Console) Test | 233 |
| Problem determination | 233 |
| Monitoring (WebSphere Business Monitor Mobile Device Console) Test | 235 |
| Problem determination | 235 |
| Policy (Tivoli Service Request Manager Maximo Console) Test | 237 |
| Problem determination | 237 |
| Security (Tivoli Access Manager) Test | 239 |
| Problem determination | 239 |
| Security (Tivoli Access Manager Web Portal Manager) Test | 240 |
| Problem determination | 240 |
| Security (WebSEAL Console) Test. | 241 |
| Problem determination | 241 |
| Web Server (IBM HTTP Server Console) Test | 242 |
| Problem determination | 242 |
| Intelligent Operations Center Event Flow Test | 243 |
| Problem determination | 243 |
| Intelligent Operations Center Notification Flow Test. | 244 |
| Problem determination | 244 |

Chapter 7. Maintaining the solution 245

| | |
|--|-----|
| Backing up data | 245 |
| Tuning performance | 246 |
| Tuning the application server | 246 |
| Tuning WebSphere Application Server | 247 |
| Managing log files. | 247 |
| Updating the LTPA token for single sign-on | 247 |
| Maintenance tips | 249 |

Chapter 8. Using the solution interface 251

| | |
|---|-----|
| Logging on | 251 |
| Logging off | 251 |
| Viewing or editing your user profile. | 252 |
| Using pages | 252 |
| Supervisor: Status view | 253 |
| Supervisor: Operations view | 254 |
| Operator: Operations view | 254 |
| Supervisor: Reports | 255 |
| Operator: Reports | 255 |
| Location Map view | 256 |
| Using portlets | 256 |
| Contacts | 257 |

| | |
|--|-----|
| Details | 257 |
| Managing events and incidents | 259 |
| Managing resources | 260 |
| Customizing the Details portlet | 260 |
| Key Performance Indicator Drill Down. | 260 |
| Location Map | 261 |
| Map controls | 262 |
| Selecting event categories for the map | 263 |
| Customizing the Location Map portlet | 263 |
| Map | 264 |
| Using the map controls | 266 |
| Selecting event categories for the map | 266 |
| Selecting resource capabilities for the map. | 266 |
| Resetting the map | 267 |
| Adding an event | 267 |
| Customizing the Map portlet | 268 |
| My Activities | 269 |
| Notifications. | 271 |
| Reports | 272 |
| Status | 274 |

Chapter 9. Troubleshooting and support 277

| | |
|--|-----|
| Techniques for troubleshooting problems | 277 |
| Enabling traces and viewing log files | 279 |
| Application server log files. | 279 |
| Enabling tracing and viewing logs on WebSphere Portal | 279 |
| Enabling tracing and viewing logs for IBM WebSphere Business Monitor on the application server | 279 |
| Event server log files | 280 |
| Enabling tracing and viewing log files for Tivoli Service Request Manager | 280 |
| Enabling tracing and viewing log files for WebSphere MQ and WebSphere Message Broker. | 281 |
| Enabling tracing and viewing log files for the Tivoli Netcool/OMNIBus XML probe | 281 |
| Enabling tracing and viewing log files for the Tivoli Netcool/OMNIBus (object server) database | 282 |
| Tivoli Netcool/OMNIBus (Process Agent) Database log file | 282 |
| Enabling and viewing Tivoli Netcool/Impact log files | 282 |
| Running the installation must gather tool | 283 |
| Troubleshooting the components | 284 |
| Installing and using IBM Support Assistant Lite | 287 |
| IBM Intelligent Operations Center messages | 287 |
| Using Knowledge bases and IBM Support. | 305 |
| Searching knowledge bases. | 305 |
| Getting fixes from Fix Central | 306 |
| Contacting IBM Support. | 306 |
| Subscribing to support updates | 307 |
| Exchanging information with IBM | 309 |
| Sending information to IBM Support | 309 |
| Receiving information from IBM Support | 309 |
| Known problems and solutions | 310 |
| Connection errors when installing IBM Intelligent Operations Center | 312 |

| | |
|--|------------|
| IPv6 networking does not start | 312 |
| Tivoli Service Request Manager does not start | 312 |
| Cannot create a new page for the user interface | 313 |
| Accessibility workarounds for portlets | 313 |
| Accessibility workaround for selecting dates in the Reports portlet | 314 |
| New events are not displayed in the Details portlet. | 314 |
| Third-party server not responding | 316 |
| Authentication mechanism not available | 316 |
| No activities are displayed in the My Activities portlet. | 317 |
| Troubleshooting with the sample data | 317 |
| Verifying the status of Tivoli Service Request Manager | 318 |
| Verifying user permissions | 319 |
| Verifying the association of a workflow with a standard operating procedure | 319 |
| Checking the log files | 320 |
| KPI data is not displayed in the Status or Key Performance Indicator Drill Down portlets | 321 |
| Events are not updated in the Status or Key Performance Indicator Drill Down portlets | 321 |
| Chapter 10. Reference | 323 |
| Products and components included with IBM | |
| Intelligent Operations Center | 323 |
| Processes running under the root account. | 324 |
| Cyber hygiene exceptions | 325 |
| File permissions requiring system administrator evaluation | 326 |
| Product and component security certifications | 327 |
| PDF library | 328 |
| Glossary | 328 |

| | |
|--|------------|
| A | 328 |
| B | 329 |
| C | 329 |
| D | 330 |
| E | 330 |
| F | 331 |
| G | 331 |
| H | 331 |
| I | 331 |
| J | 331 |
| K | 332 |
| L | 332 |
| M | 333 |
| N | 333 |
| O | 333 |
| P | 333 |
| R | 334 |
| S | 334 |
| T | 335 |
| U | 335 |
| V | 336 |
| W | 336 |
| X | 337 |
| Additional product information | 337 |
| Copyright notice and trademarks. | 339 |
| Copyright notice | 339 |
| Trademarks | 339 |
| Notices | 341 |
| Trademarks | 342 |
| Index | 345 |

Figures

Chapter 1. Solution overview

Many organizations and endeavors require efficient operational supervision and coordination. All have in common the need for the right information to be brought together so that the right people can make fast, accurate decisions and track the effect of those decisions. The IBM® Intelligent Operations Center is a software solution designed to facilitate effective supervision and coordination of operations.

Authorities face common challenges in their core systems and in making improvements to systems that are interconnected. Authorities that are forward-looking want to use the improvements in efficiency and effectiveness of smarter core systems. They adopt new ways of thinking about and using these systems. The application of advanced information technology can help authorities better understand, predict, and intelligently respond to patterns of behavior and events.

For example, IBM defines an intelligent city in terms of the improvements in quality of life and economic well-being that are achieved through applying information technologies (IT) to plan, design, build, and operate the city infrastructure. An intelligent city is not primarily about "the latest technology." It is about finding ways to use technology to make the most effective use of the existing resources, to improve the life of the citizens of the city.

The IBM Intelligent Operations Center uses the power of the real-world data generated by computer systems by:

- Collecting and managing the right data
- Integrating and analyzing that data
- Facilitating easy and timely access to information
- Presenting related information in a coherent way

The benefits of this solution are to:

- Adjust systems to achieve results based on the insights gained
- Optimize planned and unplanned operations using a holistic reporting and monitoring approach
- Build convergence of domains in an organization by facilitating communication and collaboration
- Improve quality of service and reduce expense by coordinating events

An operation can be divided into individual domains, which generally match with the organization structure and the expertise of the people involved. In a city, the expertise is held in departments, for example, in transportation, water, and public safety.

As the complexity of operations in a domain increases, a more customized solution is required. The IBM Intelligent Operations Center has a number of different integration points where customization can take place. These integration points and the infrastructure included give IBM Business Partners, service providers, and customers the flexibility to build a broad and powerful solution.

Intended audience

This product documentation is intended for people who are using, installing, administering, and maintaining the IBM Intelligent Operations Center. It also contains implementation documentation for customizing the solution and integrating the external underlying systems that IBM Intelligent Operations Center requires.

This product documentation is based on the assumption that users have prior knowledge of or proficiency in using the component products included in this solution. The product documentation is also based on the assumption that users have a basic knowledge of the Red Hat Enterprise Linux operating

system. Training for the component products or the operating system is outside the scope of this product documentation. If you require training for these products, ask your systems integrator or IBM representative where you can obtain information about base component training opportunities.

You can find links to the component product documentation in the Reference section, see the link at the end of the topic.

Related concepts:

“Additional product information” on page 337

The following additional resources are available online.

Features

The IBM Intelligent Operations Center provides measuring, monitoring, and modeling facilities that integrate underlying systems into one solution to improve operational efficiency, planning, and coordination.

The IBM Intelligent Operations Center is a solution within the IBM Smarter Cities® Software Solutions product family. The IBM Intelligent Operations Center can be installed on existing hardware (on premise) or it can be deployed in the cloud. The IBM Intelligent Operations Center can be installed by itself, or you can install it with other solutions from the IBM Smarter Cities Software Solutions product family.

The IBM Intelligent Operations Center is a GUI-based solution with role-based access to events for an organization and underlying domains. It has event management, integrated mapping, and resource monitoring capabilities. The solution can supply and track the appropriate procedures and workflow for activities in preparation for and response to events. It also has key performance indicator (KPI), reporting, and collaboration capabilities for improved effectiveness. These features provide authorities with the ability to integrate domains for improved cooperation and decision-making.

Event and incident management

The 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. Inclement weather due to arrive in the next 24 hours is a predicted event. A traffic jam is a current event affected by both the road works and weather.

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

Resource, response, and activity management

IBM Intelligent Operations Center provides a system for storing appropriate procedures and workflows based on activities associated with events. You can track the progress of workflows and monitor or update the status of activities 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.

Status monitoring

The IBM Intelligent Operations Center provides a tool for creating and displaying KPIs. The KPIs can be updated as underlying data changes. You can use this tool to:

- 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

Instant notification and messaging

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

IBM Lotus® Sametime® provides an integrated collaboration and communication tool that you can use for instant messages where and when it is needed.

Producing reports

The IBM Intelligent Operations Center has an integrated reporting facility so that you can set up and run reports with the events and KPIs supplied by the solution. You can use this facility to collect and present the information most useful to you on an up-to-date and regular basis. This facility gives you all the advantages of tailored summaries and graphical presentation.

Users and benefits

The IBM Intelligent Operations Center is designed for personnel involved with operational control in organizations, government departments, local, or city authorities: executives, supervisors, and operators.

The following table describes the users and benefits associated with using IBM Intelligent Operations Center.

Table 1. IBM Intelligent Operations Center users and benefits

| If you are a... | This software can help you... |
|-----------------|--|
| Executive | <ul style="list-style-type: none"> • Gain an executive level summary of events and incidents through maps, dashboards, alerts • Determine measures of organizational success with key performance indicators (KPIs) • Identify and track issues through reports • Direct priorities and implementation of policy based on data provided |
| Supervisor | <ul style="list-style-type: none"> • Identify and act on conflicts and issues shown on maps, dashboards, and alerts • Manage events by adding new events, editing existing events, canceling events, and escalating events to incidents • Provide information about and manage resources • Store and manage the execution of procedures and workflows associated with events • Monitor KPIs • Communicate quickly and easily on matters of importance • Design useful reports |

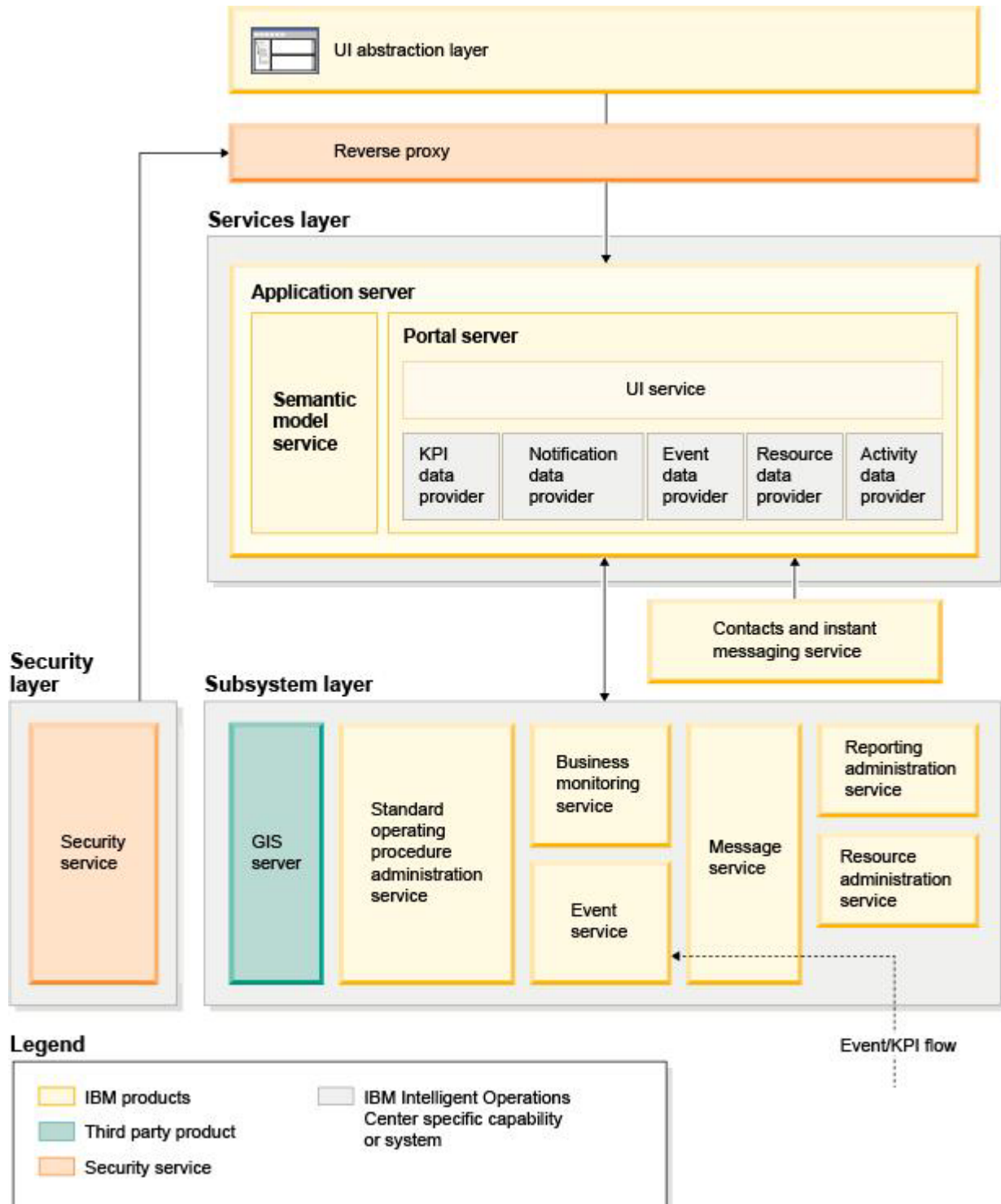
Table 1. IBM Intelligent Operations Center users and benefits (continued)

| If you are a... | This software can help you... |
|----------------------|---|
| Operator | <ul style="list-style-type: none"> • Create, edit, and monitor status events and incidents to be shown in lists • Receive and update status on assigned activities • Check available resources • Run regular and up-to-date reports • Notify, update, and issue alerts to appropriate colleagues, manager, or executives • Communicate quickly and easily in emergencies and other situations that require a response |
| User administrator | <ul style="list-style-type: none"> • Add new users and assign them to groups with the appropriate authentication • Ensure data security through category and role-based authorization groups with appropriate permissions • Set up permissions appropriate to areas of expertise and data required |
| System administrator | <ul style="list-style-type: none"> • Customize pages and portlets to suit your organization • Customize according to management requirements the events and KPIs displayed • Create and publish test events • Configure reports and distribution |

Components

At a high level, the structure of the IBM Intelligent Operations Center can be divided into major components, subsystems and services.

The following diagram shows a high-level view of the IBM Intelligent Operations Center.



UI abstraction layer

The IBM Intelligent Operations Center provides web-based, one-stop portals to event information, overall status, and details. The user interface (UI) presents customized information in various pre-configured views in common formats. All information is displayed through easy-to-use dashboards.

Security layer

All access to information is controlled by the security layer through organizational roles and data categories. This control prevents unauthorized access while enabling easy management of entitlements.

Services layer

The services layer uses common widgets and a common UI services framework to receive event data and pass it through event management to the message system. IBM Intelligent Operations Center data providers extend the UI services. Because of the variety of data that can be supplied from underlying operational systems, data is normalized according to a standard semantic reference model, which provides a common dictionary for mapping relationships. This model facilitates effect analysis and response to events without the need for multiple translations of information. The semantic model provides access to KPI and hierarchy information of underlying domains. Advanced analytics can be performed on data, identifying optimizations and predictions that can help guide decision-making and governance.

Subsystem layer

The solution provides a mediation layer to facilitate the information exchange between the solution and operational systems of underlying domains. Data from various configurable sources can be provided through gateways into a subsystem layer, which can generate alerts, KPIs and events. This integration layer enables the two-way communication of messages in various formats, open standards where possible. By using industry standard tools to transform from sources to the reference semantic model, the underlying operational systems do not need to be changed. Emergency and other response systems can be connected to the IBM Intelligent Operations Center for appropriate workflows.

The structure of the IBM Intelligent Operations Center supports:

- A central point for understanding the state of operations, managing events and incidents, and connecting domains under operations center control
- Integration with a geographic information system (GIS), location map diagram or plan for mapping events, incidents and resources spatially and visually
- Creation and monitoring of key performance indicators (KPIs), which are updated as data changes through connections to underlying domain systems
- Creation and monitoring of standard operating procedures (SOPs) with workflows and activities in association with events
- Alerts coming in from the field, including those requiring emergency or standard responses
- Collaboration capabilities, through an instant messaging facility with IBM Lotus Sametime
- Creation and distribution of up-to-date and regular reports based on event or KPI data
- A role-based security model

For more information about the IBM Intelligent Operations Center system services, see the link at the end of the topic.

Related concepts:

“IBM Intelligent Operations Center system services” on page 11
IBM Intelligent Operations Center servers provide a number of services.

Event management

The IBM Intelligent Operations Center solution focuses on the integration and optimization of information within and across multiple domains in a central operations hub, in real-time and over long periods. Event data management enables the IBM Intelligent Operations Center to assimilate data from multiple systems to constantly predict and react to significant events and trends.

Event messages are self-contained data items containing basic but complete information to which recipients can respond. Event messages are placed in queues by the IBM Intelligent Operations Center and processed by the event handling service.

Events come into the IBM Intelligent Operations Center in different forms based on the nature of the operations and domains in the central operations hub. Some examples of the forms of event are: triggers, thresholds, complex events, and manually-generated events.

Triggers are events generated by something happening and usually require an action to be taken by the recipient. Examples of triggers are:

- Fire or smoke alarms going off
- Information technology systems going down
- Intrusion detectors tripped
- Natural events picked up by sensors, such as earth tremors

The IBM Intelligent Operations Center can receive information on such events from external systems and convert it into alerts for recipients. In general, it is likely that lower level indicators would be summarized and only passed to the IBM Intelligent Operations Center if they merited wider attention. For example, all fires may not be reported as events. However, a fire involving multiple divisions of the fire service and environmental protection expertise, due to hazardous material, would merit reporting to the operations center.

Threshold events help you determine when the measurements obtained from a sensor or other source have moved outside the normal range. Basic threshold events are comparisons that compare two or more measures and report a trend. More sophisticated threshold events can compare measures against a threshold created by historical information. Examples of threshold events are:

- Over and under temperature alarms
- High and low water levels
- Air quality and water purity breaching environmental standards
- Excessive power consumption

The IBM Intelligent Operations Center can manage such events in the form of key performance indicators (KPIs).

Complex events bring together information from multiple systems to determine if a group of related events should be reported. For example, the toll road authority receives a trigger event from its monitoring system that indicates that the computer link for credit card authorization is down, followed shortly by a threshold event from the financial system warning that they are close to their credit limit for unauthorized payments. The combination of these two issues is much more serious than either in isolation, so a complex event is generated to raise awareness and coordinate a resolution.

Events that are entered manually are especially important to cities. Some of these are observed incidents, such as crimes and traffic accidents. Other examples of events entered manually are those generated from

emergency calls from citizens, from reports made by city officials, or from management systems that report on city status. The most common types of event entered manually are:

- Severe weather warnings
- Crime reports
- Fires
- Road traffic incidents – accidents, congestion, unusual loads
- Upcoming events – rock concerts, road races, parades

Complex event processing allows a city to identify exceptions to city systems easily, occasionally to identify trends from unrelated data, and to predict future issues.

What's new in version 1.5

IBM Intelligent Operations Center 1.5 introduces useful new features for the administrator and the user.

What's new for the user

With IBM Intelligent Operations Center 1.5, you can manage resources and activities associated with an event.

Manage resources and interact with location maps

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

- Assess the resources available to you in the vicinity of an event 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 clustered at the same location on a map.

 To learn more about the new Location Map portlet and enhanced Map and Details portlets, see the links at the end of the topic.

Track the status of activities associated with events

In the new My Activities portlet, you can:

- View for your group the open tasks associated with a procedure and an event.
- View the status of tasks assigned to you.
- Change the status of tasks assigned to you.

 To learn more about the My Activities portlet, see the link at the end of the topic.

Produce reports

In the new Reports portlet, you can:

- View up to six reports of events as graphs.
- Create custom reports 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 on the right side of the portlet.

 To learn more about the Reports portlet, see the link at the end of the topic.

Related concepts:

“Location Map” on page 261

Use the Location Map portlet to see events marked on a location map. A location map in the IBM Intelligent Operations Center is a map or plan with predefined areas for interaction, for example, seating areas in a major sports stadium.

“Map” on page 264

Use the Map portlet to see events and resources on a map.

“Details” on page 257

Use the Details portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

“My Activities” on page 269

The My Activities portlet displays a dynamic list of activities that are owned by the group of which the user, who is logged on to the interface, is a member.

“Reports” on page 272

Use the Reports portlet to view a report of events as a graph. The portlet provides various options to group events by, and you can choose events by a particular date or date range. These reports help you plan responses to current and future events.

What's new for the administrator

With version 1.5, you can customize your portlets and page layouts. You can also set up standard operating procedures and workflows.

Customize portlets

With the new portlet configuration options, you can set 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



To learn more about customizing portlets, see the link at the end of the topic.

Manage events with standard operating procedures and workflows

You can define procedures and activities associated with events:

- Define standard operating procedures based on a job plan.
- Create workflows.
- Define parameters for the selection of a standard operating procedure based on the parameters of an event.



To learn more about associating activities associated with events, see the standard operating procedure link at the end of the topic.

Script and publish events

You can use the new Event Scripting portlet to create a sequential list of events to be published at predefined time intervals.



To learn more about scripting and publishing events, see the link at the end of the topic.

Check service status

You can use the new System Verification Check tool to check the operational status of IBM Intelligent Operations Center services.

 To learn more about the System Verification Check tool, see the link at the end of the topic.

Support protocols

The IBM Intelligent Operations Center now supports events with protocols other than the Common Alerting Protocol. You 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.

 To learn more about integration points and protocols, see the link at the end of the topic.

Related concepts:

“Standard Operating Procedures” on page 123

You can define standard operating procedures and activities to manage events that come into the IBM Intelligent Operations Center. Use the Standard Operating Procedures portlet to access the standard operating procedure, standard operating procedure selection matrix, and workflow designer applications in Tivoli[®] Service Request Manager[®].

“Event Scripting” on page 103

Use the Event Scripting portlet to write a script to create a sequential list of events to be published at predefined time intervals.

“Verifying the components” on page 199

The System Verification Check tool tests components within IBM Intelligent Operations Center to determine if they are accessible and operational.

“Integration points and protocols” on page 87

Other systems can be integrated with the solution through the IBM Intelligent Operations Center services and policies. Data can be received in the Common Alerting Protocol (CAP) format; other protocols are also supported.

Related tasks:

“Customizing the portlets” on page 139

As an administrator you can change the portlet settings to customize a portlet.

Chapter 2. Installing and configuring

IBM Intelligent Operations Center provides a deployment wizard that installs the environment required by the IBM Intelligent Operations Center. After deploying the environment and the IBM Intelligent Operations Center package, some additional configuration is required.

Preparing for installation

Before deploying IBM Intelligent Operations Center, understand the IBM Intelligent Operations Center system configuration and ensure that the prerequisites are met for the environment.

IBM Intelligent Operations Center system services

IBM Intelligent Operations Center servers provide a number of services.

Analytics services

Provides data analysis and presentation services.

Application server

Provides Java Enterprise Edition services supporting the product.

Security

Provides services determining if a user is authorized to use the system and defining their privileges within the system.

Authorization services

Provides services determining the services a user is authorized to use.

Business monitoring

Provides aggregation, analysis, and presentation of business process and activity information in real-time.

Instant messaging server

Provides real-time collaboration capabilities for users and applications.

Configuration services

Manages the product configuration including inventory and change management.

Database

Provides the database manager for application and system data.

Directory

Provides the mapping between names and values. Data services is used as a repository for user names and passwords.

Event handling

Collects, aggregates, presents, and handles system events.

Messaging services

Provides message and workflow services to the product.

Monitoring services and agents

Provides monitoring activity within the product.

Portal

Provides services supporting user interaction with the product.

Semantic model

Provides services allowing applications to model real world objects and relationships.

Related concepts:

“Components” on page 5

At a high level, the structure of the IBM Intelligent Operations Center can be divided into major components, subsystems and services.

IBM Intelligent Operations Center hardware requirements

Five servers meeting minimum requirements are required to install IBM Intelligent Operations Center.

The servers must be 64-bit x86 servers.

The minimum requirements servers used by IBM Intelligent Operations Center are shown in Table 2. The recommended minimum disk space does not include space for boot and swap partitions.

Table 2. Minimum hardware requirements

| Resource | Application server | Event server | Data server | Management server | Installation server |
|--|--------------------|--------------|-------------|-------------------|---------------------|
| CPUs | 4 | 4 | 4 | 4 | 2 |
| Memory | 24 GB | 16 GB | 16 GB | 24 GB | 4 GB |
| Network adapters | 1 | 1 | 1 | 1 | 1 |
| Disk space | 113 GB | 108 GB | 108 GB | 108 GB | 108 GB |
| Additional disk space required during installation | 90 GB | 90 GB | 90 GB | 90 GB | 90 GB |

The minimum requirements for the directories on each server, excluding space required for the boot and swap partitions is shown in Table 3.

Table 3. Minimum space requirements for each directory

| Directory | Minimum space | Notes |
|---------------|----------------|---|
| / | 8 GB | |
| /opt | 35 GB or 40 GB | 40 GB is required for the application server, 35 GB is required for all other servers |
| /usr | 8 GB | |
| /home | 5 GB | |
| /tmp | 10 GB | |
| /chroot | 1 GB | |
| /datahome | 25 GB | |
| /loghome | 8 GB | |
| /installMedia | 90 GB | This directory can be deleted after installation. |
| /var | 8 GB | |

Related tasks:

“Preparing the servers” on page 17

Before installing IBM Intelligent Operations Center, validate that server configuration requirements are satisfied. The precheck tool will verify that many of these requirements have been implemented.

Related information:

 System requirements

Prerequisite software requirements

Before installing IBM Intelligent Operations Center, the servers must have the appropriate software installed.

IBM Intelligent Operations Center requires Red Hat Enterprise Linux (RHEL) 5 Server x86-64 Update 5 or later to be installed on all servers. Red Hat Enterprise Linux Version 6 is not supported.

Related tasks:

“Preparing the servers” on page 17

Before installing IBM Intelligent Operations Center, validate that server configuration requirements are satisfied. The precheck tool will verify that many of these requirements have been implemented.

Related information:

 System requirements

Supported browsers

The IBM Intelligent Operations Center solutions interface supports a number of browsers. Some browsers can be used with limitations.

IBM Intelligent Operations Center has been tested, and is supported, on the following browsers:

- Microsoft Internet Explorer 8.x (32-bit only)
- Microsoft Internet Explorer 9.x (32-bit only)
- Mozilla Firefox 10 ESR

Internet Explorer Compatibility View

IBM Intelligent Operations Center does not support Internet Explorer 8 or Internet Explorer 9 Compatibility View.

Note: Compatibility View may be switched on temporarily, if you encounter a problem when creating a new page for the user interface, see the link at the end of the topic for details.

Internet Explorer 8.x performance

Users might experience slow performance using Internet Explorer 8.x.

To avoid this problem, use Internet Explorer 9.x or Firefox 10 ESR.

Minimum screen resolution

IBM Intelligent Operations Center is designed to run at a minimum 1280 x 800 screen resolution.

Related tasks:

“Cannot create a new page for the user interface” on page 313

Resolve a problem which occurs when creating a new page if you are working with Microsoft Internet Explorer 9.

Media packaging

IBM Intelligent Operations Center can be ordered as a package of DVDs or can be obtained through Passport Advantage®.

The product number is 5725-D69.

Related information:

 [Passport Advantage](#)

 [Download IBM Intelligent Operations Center Version 1.5 image files](#)

Installation checklists

Installation checklists are available for the two different installation options for IBM Intelligent Operations Center. These checklists provide an overview of the installation steps and can be used to track the installation progress.

Checklist - installing using IBM Installation Manager

Use this checklist to track the installation steps when installing IBM Intelligent Operations Center using IBM Installation Manager.

About this task

A printable version of this checklist is available using the related link at the end of this topic.

Procedure

- ___ 1. Make sure you have the necessary hardware.
- ___ 2. Make sure the required software is installed on the hardware.
- ___ 3. Prepare the servers.
- ___ 4. Copy the installation package to the installation server.
- ___ 5. Install the Java runtime environment.
- ___ 6. Install IBM Installation Manager.
- ___ 7. Restart IBM Installation Manager and install the **Configure topology** package.
- ___ 8. Restart IBM Installation Manager and install the **Prepare target servers** package. If this step completes successfully, skip step 9.
- ___ 9. Restart IBM Installation Manager and install the **Ignore system check errors** package. When running IBM Installation Manager after resolving system check errors, or after determining that the installation can continue, select both **Prepare target servers** and **Ignore system check errors** on the second run.
- ___ 10. Restart IBM Installation Manager and install the **Prepare Environment** package.
- ___ 11. Restart IBM Installation Manager and install the **Install and Configure Platform - Part 1** package.

Tip: Do not select both Part 1 and Part 2 at the same time. These steps will take the longest time to run. If both are run together, and there is a failure, then both will need to be rerun; even if one was successful.

Important: Do not shut down the servers between installation phases. Shutting the servers down between phases has not been tested and can result in unpredictable results.

- __ 12. Restart IBM Installation Manager and install the **Install and Configure Platform - Part 2** package.
- __ 13. Restart IBM Installation Manager and install the **Install Platform Control Tool** package.
- __ 14. Restart IBM Installation Manager and install the **Install System Verification Check Tool** package.
- __ 15. Restart all IBM Intelligent Operations Center servers.
 - a. Shut down all IBM Intelligent Operations Center servers using the Platform Control Tool.
 - b. Shut down and restart all servers from the operating system.
 - c. Start all IBM Intelligent Operations Center servers using the Platform Control Tool.
- __ 16. Restart IBM Installation Manager and install the **Install Application** package. This will install the IBM Intelligent Operations Center application.
- __ 17. Configure the IBM Intelligent Operations Center architecture.
 - __ a. Configure collaboration services if you are using IPv6.
 - __ b. Configure single sign-on for collaboration services.
 - __ c. Install and configure semantic model services.
 - __ d. Configure the Platform Control Tool.
 - __ e. Encrypt the Tivoli Service Request Manager administrative password.
 - __ f. Set the minimum number of threads for the EventProcessor.
 - __ g. Change the Default and WebContainer thread pool size.
- __ 18. Install any other applications.
- __ 19. Restart IBM Installation Manager and install and run the **Cyber Hygiene** package. Cyber hygiene provides additional security to the IBM Intelligent Operations Center system.

Note: Cyber Hygiene is installed and run in the same step.
- __ 20. Configure users requiring ssh access and passwords.

Results

The IBM Intelligent Operations Center architecture and IBM Intelligent Operations Center application are installed and ready for use.

What to do next

A must gather tool is provided to collect installation logs to help diagnose installation issues.

Related concepts:

“Cyber hygiene overview” on page 76

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Related information:



Printable version of this checklist

Checklist - installing step-by-step

Use this checklist to track the installation steps when installing IBM Intelligent Operations Center using scripts and commands.

About this task

A printable version of this checklist is available using the related link at the end of this topic.

Procedure

- ___ 1. Make sure you have the necessary hardware.
- ___ 2. Make sure the required software is installed on the hardware.
- ___ 3. Prepare the servers.
- ___ 4. Install the Java runtime environment.
- ___ 5. Copy the installation package to the installation server.
- ___ 6. Unpack and prepare the installation package.
- ___ 7. Define the installation properties.
- ___ 8. Define the topology for the installation by editing the topology properties file.
- ___ 9. Generate the topology password which will be used to encrypt key files.
- ___ 10. Generate the topology file.
- ___ 11. Run the Precheck tool to verify the environment is ready to install IBM Intelligent Operations Center.
- ___ 12. Configure Linux security settings by using the provided tool or by running a series of commands.
- ___ 13. Install the IBM Intelligent Operations Center architecture. This can be done in one phase or in three phases. If running in a virtualized environment, installing in multiple phases allows you to create a snapshot between the installation phases.
 - Install IBM Intelligent Operations Center in one phase. Installation will take up to 14 hours.
 - Install IBM Intelligent Operations Center in three phases. The three phases are:
 - a. Copy the installation files from the installation server to the target servers. This phase takes approximately 2 hours.
 - b. Install the first phase of the topology. This phase takes approximately 9 hours.
 - c. Install the second phase of the topology. This phase takes approximately 3 hours.

Important: Do not shut down the servers between installation phases. Shutting the servers down between phases has not been tested and can result in unpredictable results.

- ___ 14. Install the Platform Control Tool.
- ___ 15. Install the System Verification Check tool.
- ___ 16. Verify that the IBM Intelligent Operations Center architecture is correctly installed.
- ___ 17. Configure the IBM Intelligent Operations Center architecture.
 - ___ a. Configure collaboration services if you are using IPv6.
 - ___ b. Configure single sign-on for collaboration services.
 - ___ c. Install and configure semantic model services.
 - ___ d. Encrypt the Tivoli Service Request Manager administrative password.
 - ___ e. Set the minimum number of threads for the EventProcessor.
 - ___ f. Change the Default and WebContainer thread pool size.
- ___ 18. Install the IBM Intelligent Operations Center application.
- ___ 19. Install any other applications.
- ___ 20. Install and run cyber hygiene. Cyber hygiene provides additional security to the IBM Intelligent Operations Center system.

Note: Cyber hygiene is installed and run in the same step.
- ___ 21. Configure users requiring ssh access and passwords.

Results

The IBM Intelligent Operations Center architecture and IBM Intelligent Operations Center application are installed and ready for use.

What to do next

A must gather tool is provided to collect installation logs to help diagnose installation issues.

Related concepts:

“Cyber hygiene overview” on page 76

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Related information:



Printable version of this checklist

Preparing the servers

Before installing IBM Intelligent Operations Center, validate that server configuration requirements are satisfied. The precheck tool will verify that many of these requirements have been implemented.

About this task

If running in a virtual environment, using a template for these steps can help reduce setup time.

Procedure

1. Ensure that the servers meet the hardware and software requirements.
2. Set up TCP/IP networking.
 - a. Define a fully-qualified name and short host name using a DNS server or by definition in the `/etc/hosts` file.
 - b. Verify the TCP/IP configuration. The servers are correctly configured if the following tests complete successfully.
 - 1) The `hostname -s` command returns the defined short host name for the server.
 - 2) The `hostname -f` command returns the fully qualified domain and host name for the server.
 - 3) The `hostname -d` command returns the domain name of the server.
 - 4) The results of a `ping` command, or `ping6` command for IPV6 environments, with the short host name for each server indicates that the server is accessible.
 - 5) The results of a `ping` command, or `ping6` command for IPV6 environments, with the fully-qualified name for each server indicates that the server is accessible.
 - c. Enable local loopback addressing for each server in the `/etc/hosts` file.
 - d. Verify local loopback addressing. The servers are correctly configured if the following tests complete successfully.
 - 1) The `ping -n localhost` command returns the address `127.0.0.1`.
 - 2) The `ping -n localhost.localdomain` command returns the address `127.0.0.1`.
 - 3) The `ping6 -n localhost6` command in an IPV6 environment returns the address `::1`.
 - 4) The `ping6 -n localhost6.localdomain6` command in an IPV6 environment returns the address `::1`.
 - e. Make sure the ports required by IBM Intelligent Operations Center are available. The ports required for each server are shown in Table 4 on page 18.

Table 4. Ports required for product use

| Server | Ports required for product use |
|-------------|--|
| Application | 80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016 |
| Event | 80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016 |
| Data | 389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008 |
| Management | 80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001 |

f. Make sure the maximum open file descriptors defined by the **nofile** parameter in the `/etc/security/limits.conf` file is set to 20480 for the following servers:

- Application server
- Event server
- Data server
- Management server

This is done by adding the following lines to the `/etc/security/limits.conf` file:

```
* soft nofile 20480
* hard nofile 20480
```

This will set the soft (default) limit of the number of open files for all users to 20480, and also set the hard (maximum) limit for all users to 20480. You might want to increase the hard limit if other applications require more than 20480 files.

g. Add or update the **net.ipv4.tcp_fin_timeout** parameter in the `/etc/sysctl.conf` file to 30 for the following servers:

- Application server
- Event server
- Data server
- Management server

3. Disable all Linux firewalls.

4. Disable SELinux (Security Enforcing Linux) by editing the `/etc/selinux/config` file and changing SELINUX to disabled. After changing the configuration, reboot the server.

5. Ensure that all servers have the same time and date set as indicated by the Linux operating system. A time synchronization service can be used.

6. Enable the `sshd` service on each server by running the `/etc/init.d/sshd start` command. The service needs to be enabled for root login with password authentication. TCP/IP port 22 must be configured in the operating system as an available ssh access port for use during installation processing. The TCP/IP port number for Platform Control Tool ssh access is specified in the topology properties file. Only the Platform Control Tool uses the configured port.
7. Install the Linux packages in Table 5 on each server using the `yum install package_name` command. These packages are available from Red Hat.

Table 5. Required and optional Linux packages for IBM Intelligent Operations Center target servers

| Package | Application server | Data server | Event server | Management server |
|------------------------|--------------------|-------------|--------------|-------------------|
| compat-libstdc++-33-3* | required | required | required | required |
| libXp-1.0.0-8* | required | optional | required | required |
| libXmu-1* | required | optional | required | required |
| libXtst-1* | required | optional | required | required |
| pam-0* | required | optional | optional | optional |
| rpm-build-4* | required | optional | optional | required |
| libaio-0* | required | required | optional | required |
| libstdc++-4* | required | required | required | required |
| libXft-2* | required | optional | optional | required |
| compat-db-4* | required | optional | optional | required |
| elfutils-libs-0* | required | optional | optional | required |
| elfutils-0* | required | optional | optional | required |
| libgcc-4* | required | optional | required | optional |
| compat-glibc-2* | required | optional | required | optional |
| openmotif22-2* | required | optional | required | optional |
| audit-libs-1* | required | optional | optional | optional |
| glibc-2* | required | optional | optional | optional |
| glibc-common-2* | required | optional | optional | optional |
| glibc-headers-2* | optional | required | optional | required |
| glibc-devel-2* | optional | required | optional | required |
| compat-gcc* | optional | required | optional | required |
| libXft-2* | optional | optional | required | optional |
| libXpm-3* | optional | optional | required | optional |
| xorg-x11-xauth* | optional | optional | required | optional |
| ksh-* | optional | optional | optional | required |

The following commands can be used to install the required packages on each server. If the package is already installed, it will not be reinstalled.

Application server

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0*
rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0*
elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2*
glibc-common-2*
```

Data server

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2*  
glibc-devel-2* compat-gcc*
```

Event server

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4*  
libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

Management server

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4*  
libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0*  
glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Make sure Java 1.6 is not installed on any of the servers:

- Installation server
- Application server
- Event server
- Data server
- Management server

Related concepts:

“Prerequisite software requirements” on page 13

Before installing IBM Intelligent Operations Center, the servers must have the appropriate software installed.

“IBM Intelligent Operations Center hardware requirements” on page 12

Five servers meeting minimum requirements are required to install IBM Intelligent Operations Center.

Related tasks:

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

Related information:

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

TCP/IP networking

Prior to installing IBM Intelligent Operations Center, TCP/IP networking between the servers must be correctly set-up.

All servers, including the installation server, used by IBM Intelligent Operations Center must be configured with a short host name and a fully-qualified host name. The host names must resolve on each server to the correct IP address. Configuration can be done using a DNS server or by adding definitions to the `/etc/hosts` file.

The fully-qualified host name for each server must have at least three components. For example: `myhost.mydomain.com` where the top level domain is a standard Internet top-level domain.

Important: Short host names and fully-qualified host names must be specified in the correct case. For example, `MyCompany.MyDomain.com` cannot be specified as `mycompany.mydomain.com`.

IPv6 networking is supported by IBM Intelligent Operations Center, but IPv4 must be installed and configured as well. IPv4 addresses do not need to be assigned to the servers, but the IPv4 loopback address (`127.0.0.1`) must be enabled and the `localhost` host name must resolve to `127.0.0.1`.

Configuration changes are shown in Table 6 on page 21. These are guidelines for setting up TCP/IP networking on the IBM Intelligent Operations Center installation server and target servers by editing the Linux network configuration files. The configuration notes in Table 6 on page 21 are only guidelines. Any network setup conforming to the requirements described previously should work.

Table 6. TCP/IP configuration guidelines

| File | Notes |
|------------|---|
| /etc/hosts | <p>The hosts file resolves TCP/IP names to IP addresses. If the configuration does not have a DNS server, all servers and their IP addresses, short host names, and fully-qualified names must be defined in this file. Local loopback addresses and host names are also defined in this file.</p> <p>If a DNS server is being used, hosts which are resolved by the DNS do not need to be included in this file.</p> <p>Important: When using IPv4, the local loopback address 127.0.0.1 must be mapped to the localhost and localhost.localdomain host names.</p> <p>The following is a sample /etc/hosts file using IPv4 addresses.</p> <pre># local loopback definitions -- do not remove # or alter these! 127.0.0.1 localhost.localdomain localhost # use the following if IPv6 is enabled in your # network definitions ::1 localhost6.localdomain localhost6 # installation server 192.168.0.205 IOC15Install.IOC15.com IOC15Install # target runtime servers 192.168.0.211 IOC15App.IOC15.com IOC15App 192.168.0.212 IOC15Event.IOC15.com IOC15Event 192.168.0.213 IOC15DB.IOC15.com IOC15DB 192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt</pre> <p>Use IPv6 address notation to assign IPv6 static addresses</p> <p>.</p> <p>Both IPv6 and IPv4 addresses can be defined on the same server.</p> |

Table 6. TCP/IP configuration guidelines (continued)

| File | Notes |
|---|--|
| /etc/sysconfig/network-scripts/ifcfg- <i>adapter_name</i> | <p>The <i>ifcfg-adapter_name</i> file defines the basic network settings for the specified network adapter. The Linux assigned name for the network adapter is specified by <i>adapter_name</i>. The typical value for <i>adapter_name</i> is eth0 but might be different for your environment.</p> <p>For IPv4 networking the following parameters should be defined.</p> <p>IPADDR Specify the IPv4 IP address of the server being configured.</p> <p>NETMASK Specify the IPv4 network mask of the server being configured.</p> <p>GATEWAY Specify the IPv4 default network IP address of the server being configured.</p> <p>BOOTPROTO If static IP addressing is being used, specify none.</p> <p>NM_CONTROLLED Specify no to disable the Network Management service from modifying the <i>ifcfg-adapter_name</i> file.</p> <p>ONBOOT Specify yes to start the adapter automatically.</p> <p>IPV6INIT Specify yes if the adapter is to use IPv6 networking.</p> <p>IPV6ADDR Specify the server IPv6 IP address if IPV6INIT=yes is specified.</p> <p>IPV6_DEFAULTGW Specify the server IPv6 default network gateway IP address if IPV6INIT=yes is specified.</p> |
| /etc/sysconfig/network | <p>The network file specifies general networking parameters.</p> <p>For IPv4 networking the following parameters should be defined:</p> <p>NETWORKING Specify yes to enable IPv4 networking.</p> <p>NETWORKING_IPV6 Specify yes if IPv6 networking is also desired.</p> <p>HOSTNAME Specify the server short host name.</p> |

Table 6. TCP/IP configuration guidelines (continued)

| File | Notes |
|--------------------|---|
| /etc/resolv.conf | <p>The <code>resolv.conf</code> file is used to define DNS servers for the network and a default search domain. If DNS servers are not being used, this file should be empty.</p> <p>If a DNS server is used, the <code>resolv.conf</code> should contain the following lines:</p> <pre>search domain_name nameserver first_DNS_server nameserver second_DNS_server</pre> <p>For example:</p> <pre>search yourcompany.com nameserver 10.75.20.10 nameserver 10.75.20.11</pre> <p>The search value specifies the default search domain. The first <code>nameserver</code> value is the IP address of the DNS server. A second <code>nameserver</code> value can be used to specify a secondary DNS server. The second <code>nameserver</code> specification is optional.</p> |
| /etc/modprobe.conf | <p>The <code>modprobe.conf</code> file defines configuration options for modules loaded in the system.</p> <p>IPv6 networking might require that the following lines be commented out and the server rebooted:</p> <pre>alias ipv6 off options ipv6 disable=1</pre> |

When correctly configured, each server must successfully pass the following tests:

1. The `hostname -s` command returns the defined short host name for the server.
2. The `hostname -f` command returns the fully qualified domain and host name for the server.
3. The `hostname -d` command returns the domain name of the server.
4. The results of a `ping` command, or `ping6` command for IPV6 environments, with the short host name for each server indicates that the server is accessible.
5. The results of a `ping` command, or `ping6` command for IPV6 environments, with the fully-qualified name for each server indicates that the server is accessible.

Related tasks:

“Preparing the servers” on page 17

Before installing IBM Intelligent Operations Center, validate that server configuration requirements are satisfied. The precheck tool will verify that many of these requirements have been implemented.

“IPv6 networking does not start” on page 312

If IPv6 networking does not start on a server, the `/etc/modprobe.conf` file might require changes.

“Running the Precheck tool” on page 40

Before uploading installation packages to the target servers, check that the target servers are ready for the installation by running the Precheck tool.

Copying the installation package to the installation server

Copy the IBM Intelligent Operations Center installation package to the installation server before installing the product.

Before you begin

Before copying the installation package to the installation server, make sure all the servers have been properly prepared.

Procedure

1. Create a directory on the installation server for the installation files, for example, `/installHome`.
2. Make note of full path to the created directory. For example, if the created directory is `installHome` for the `ibmadmin` user, the full path would be `/home/ibmadmin/installHome`. This directory path is referred to as *install_home* in other installation directions.
3. For each physical DVD, or ISO image downloaded from Passport Advantage, do the following.
 - a. Create a directory to mount the DVD. For example, run the `mkdir /mnt/ba15` command.
 - b. Mount the DVD. For example, when using an ISO image, run the `mount -o loop ISO_directory/ISO_filename /mnt/ba15` command where *ISO_directory* is the location of the ISO image and *ISO_filename* is the ISO file .
 - c. Copy the DVD contents to the directory created in step 1. For example, when using an ISO image, run the `cp /mnt/ba15/* install_home` command.
 - d. Unmount the DVD. For example, when using an ISO image, run the `umount /mnt/ba15` command.
4. Change to the *install_home* directory.
5. Run the `ba15_media_prep.sh combine` command. This command must be run before performing any other installation steps.

Note: If your *install_home* directory is something other than `/installMedia`, edit the `ba15_media_prep.sh` file and change the `MEDIA_BASE` value to your designated *install_home* directory before running the script.

This command combines files that are split across DVDs or ISO images.

Related concepts:

“Installation media location” on page 29

The IBM Installation Manager allows the installer to specify where the installation packages are located during the installation of the IBM Intelligent Operations Center.

Related tasks:

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

“Installing the Java runtime environment”

The Java 6 runtime environment must be installed on the installation server before installing IBM Intelligent Operations Center.

Installing the Java runtime environment

The Java 6 runtime environment must be installed on the installation server before installing IBM Intelligent Operations Center.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as `root` or switch to the root account by running the `su -` command.
2. Change to the directory where the IBM Intelligent Operations Center installation files were copied.
3. Run the `yum --nogpgcheck install install_media/ibm-java-x86_64-jre-6.0-10.1.x86_64.rpm` command.

4. Run the `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` command.
5. Verify the Java environment by running the `echo $JAVA_HOME` command and confirming that `/opt/ibm/java-x86_64-60/jre` is returned.

Related tasks:

“Copying the installation package to the installation server” on page 23

Copy the IBM Intelligent Operations Center installation package to the installation server before installing the product.

“Configuring the Platform Control Tool” on page 56

After installing IBM Intelligent Operations Center, if you have installed a Java™ JRE different from the one provided with IBM Intelligent Operations Center, you need to define the JRE location used by the Platform Control Tool.

“Installing IBM Intelligent Operations Center using Installation Manager”

IBM Intelligent Operations Center can be installed using the provided graphical installer.

Installing IBM Intelligent Operations Center using Installation Manager

IBM Intelligent Operations Center can be installed using the provided graphical installer.

Before you begin

The product package needs to be copied to the installation server in the *install-home* directory before following these steps.

About this task

A progress indicator is displayed during the installation. However, since installation tasks are run remotely on the target servers, the progress indicator does not indicate the true time remaining for the installation. “Installation components” on page 28 provides the installation time estimated for each component.

If you want to cancel the installation at any point, click **Cancel** in the IBM Installation Manager user interface.

Important: Do not run the `launchpad.sh` command after the first component is successfully installed. You will not be given the option to modify your installation. Use the `/opt/IBM/InstallationManager/eclipse/IBMIM` command to restart the installer instead as noted in step 24 on page 26.

Procedure

1. Run the `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` command.
2. Extract the `BA_1.5_GUI_Installer_Lite_Launchpad.zip` file in *install_home*.
3. Start the installation launchpad by running the `install_home/launchpad.sh` command.
4. Install IBM Installation Manager.
 - a. Click **Install IBM Installation Manager**.
 - b. Click **Next**.
 - c. Read the license information.
 - d. If you agree to the license terms, select I accept the terms in the license agreement and click **Next**. The installation will continue.
 - e. If you do not agree to the license terms, select I do not accept the terms in the license agreement and click **Next**. The installation will terminate.
 - f. Select where IBM Installation Manager will be installed.
 - g. Click **Next**.
 - h. Click **Install**.

- i. Restart the IBM Installation Manager.
IBM Installation Manager is installed.
5. After the IBM Installation Manager is installed, the IBM Installation Manager needs to be closed and restarted. Starting IBM Installation Manager from the launchpad will pick up the topology file for IBM Intelligent Operations Center.
6. Click **Install IBM Intelligent Operations Center**.
7. Select the IBM Intelligent Operations Center - Version 1.5 package.
8. Click **Next**.
9. Read the license information.
 - a. If you agree to the license terms, select I accept the terms in the license agreement and click **Next**. The installation will continue.
 - b. If you do not agree to the license terms, select I do not accept the terms in the license agreement and click **Next**. The installation will terminate.
10. Specify the Shared Resource Directory for the installation. This directory will be used any time you use the IBM Installation Manager to install products using the installation server. Make sure to specify a drive with the most available space on the server.
11. Click **Next**.
12. Create a new package group by selecting Create a new package group. Select IBM Intelligent Operations Center.
13. Specify the name of the Installation Directory. The Installation Directory will be created. The installer will create subdirectories under this directory as needed.
14. For Architecture Selection, select 64-bit.
15. Click **Next**.
16. Deselect all options.
17. Select **Configure topology**.
18. Click **Next**.
19. Enter the configuration options. Make note of any defined passwords.
20. Click **Next**.
21. Review the installation options and click **Next** to start the installation.
22. After the installation completes, close IBM Installation Manager and the launchpad. Do not close the terminal window where the launchpad was started in step 3 on page 25 since it has the JAVA_HOME environment set. If the terminal window is closed, JAVA_HOME must be exported again before continuing.
23. If the value entered for the topology password is greater than 15 characters in length, do the following to define a password for ITM.ADMIN.USER.PWD that is 15 characters or less in length.
 - a. On the installation server edit the *install_home/ioc/topology/iop_lite_topo.properties* file where *install_home* is the directory where the IBM Intelligent Operations Center installation package was copied.
 - b. Change the value defined for the ITM.ADMIN.USER.PWD to a value 15 characters or less. This password will be used when logging in the sysadmin user instead of the topology password.
 - c. Save the changes.
24. Start the IBM Installation Manager by running the **/opt/IBM/InstallationManager/eclipse/IBMIM** command.
25. Click **Modify > Next**.
26. Select **Prepare target servers**.
27. Click **Next > Modify**.

28. If there are errors, review the log files in the `/var/ibm/InstallationManager/logs/native` directory. The log file names begin with a timestamp that can be used to correlate the log to when the installation tool was run.
29. Correct any errors or warnings found in the logs pertaining to your system and finish the installation before installing the next component. Some warnings and errors can be ignored. For example, warnings about IPv6 if you do not have IPv6 enabled or if your configuration is not connected to a Domain Name Service (DNS).
30. After correcting any errors, return to step 25 on page 26. You will have the option to ignore system check errors. Select the next component in the list in step 26 on page 26. Continue the process until cyber hygiene is to be installed.

Important: Do not shut down the servers between installation phases. Shutting the servers down between phases has not been tested and can result in unpredictable results.

Cyber hygiene applies best practice configurations to provide additional security to the IBM Intelligent Operations Center system. Before installing cyber hygiene, complete the post-installation configuration. Once the post-installation configuration is complete, return to step 24 on page 26 and install and run cyber hygiene. Components successfully installed when IBM Installation Manager was previously run are checked. Do not uncheck these components or the components will be uninstalled when IBM Installation Manager is run again.

If running in a virtualized environment, take a snapshot with memory of all servers after an installation step successfully complete and before installing the next component. This snapshot can be used to restart the installation at a successful state should an error occur.

To reduce the time cyber hygiene runs scans and remediation, unmount any file system not required to be assessed for security. For example, the `install_media` directories on each server can be deleted after all installation steps are complete. These directories can be deleted or unmounted before running cyber hygiene.

Note: Cyber hygiene is installed and run in the same step.

Cyber hygiene should be the last step before moving your system to production status or when your system must address good security practices. All applications and solutions should be installed and configured before running cyber hygiene so the final system can be scanned and remediations applied.

Changes applied to the system by cyber hygiene can cause problem with other applications and solutions. For example, other applications and solutions might have requirements on the Linux environment that are not in accord with good security practices. An application or solution might require for the system to be logged on as the root user to be installed or run. In this case some of the cyber hygiene changes might need to be temporarily or permanently changed or another solution found from the supplier of the application or solution.

Once cyber hygiene changes are made, there is no automated method to change them. Any changes must be made by manual updates to the Linux operating system or by changing file or directory permissions.

Related concepts:

“Removing installation services from the production system” on page 64

After installing IBM Intelligent Operations Center, the installation services can be removed from the production system servers. It is suggested that the installation server be kept since some of its services might be required for maintenance activities.

“Post-installation IBM Intelligent Operations Center configuration” on page 49

After installing the IBM Intelligent Operations Center architecture using Installation Manager or step-by-step, several post-installation configuration steps need to be done to complete the installation.

“Cyber hygiene overview” on page 76

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Related tasks:

“Preparing the servers” on page 17

Before installing IBM Intelligent Operations Center, validate that server configuration requirements are satisfied. The precheck tool will verify that many of these requirements have been implemented.

“Verifying the installation” on page 48

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

“Copying the installation package to the installation server” on page 23

Copy the IBM Intelligent Operations Center installation package to the installation server before installing the product.

“Installing the Java runtime environment” on page 24

The Java 6 runtime environment must be installed on the installation server before installing IBM Intelligent Operations Center.

Installation components

IBM Intelligent Operations Center is installed as seven components.

Table 7. IBM Intelligent Operations Center installation components

| Component | Estimated installation time | What is installed |
|------------------------------------|---|--|
| Prepare Install | Precheck: 10 minutes Upload: 2 hours | The server environment is checked that it meets minimum requirements and the files required for the installation are copied to the target servers. |
| Prepare Environment | 10 minutes | Updates the /etc/sudoers and ~/.ssh/known_hosts files as required for IBM Intelligent Operations Center |
| Install and Configure Platform | Phase 1: 12 hours Phase 2: 3 hours | The required platform is installed on the target servers. The installation is done in two phases. |
| Platform Control Tool | 10 minutes | Tools required to start, stop, and query the status of IBM Intelligent Operations Center servers are installed on the Management server. |
| Platform System Verification Check | 15 minutes | Tools used to determine if key platform capabilities are installed on the Application server. |
| Application | 3 hours | The IBM Intelligent Operations Center application is installed on the target servers. |
| Cyber hygiene | up to 1.5 hours | Capabilities for mitigation and remediation of known cyber security exposures are installed on the target servers. The processing time is determined by the speed of the hardware and if extra, unnecessary files are on the target servers. |

Configuration options

The IBM Installation Manager allows the installer to specify configuration options during the installation of the IBM Intelligent Operations Center.

Topology password

The IBM Installation Manager allows the installer to specify the passwords to be used with the IBM Intelligent Operations Center.

The installer can specify the passwords shown in Table 8.

Table 8. IBM Intelligent Operations Center passwords

| Password | Description |
|---------------------|--|
| Topology password | <p>The topology password is the password used for all accounts created by the IBM Intelligent Operations Center installer except for those passwords specifically requested during the installation process and the <code>icsystemuser</code> password which is defined as <code>passwd</code> and cannot be changed. The topology password also protects the secret key created by the <code>createSecretKey</code> command.</p> <p>The password for one account cannot exceed 15 characters. If the topology password is greater than 15 characters in length, special configuration steps need to be taken to redefine the password for this account.</p> |
| Admin user password | The administrator password set for the Linux user <code>ibmadmin</code> . This user is used by the Platform Control Tool when managing the target server components. |
| Encryption seed | <p>The encryption seed value is used to encrypt user passwords and other sensitive data within the database. The encryption seed must be a 12 to 1016 printable ASCII character value.</p> <p>A strong string should be used. For example, a long string comprised of mixed-case letters, number and special characters without common words or phrases.</p> |
| Encryption salt | The encryption salt value is used to encrypt user passwords and other sensitive data within the database. The encryption salt must be a 12 printable ASCII character value between code points 33 and 126. |

Installation media location

The IBM Installation Manager allows the installer to specify where the installation packages are located during the installation of the IBM Intelligent Operations Center.

The installer can specify the installation directories shown in Table 9.

Table 9. IBM Intelligent Operations Center installation directories

| Directory | Description | Recommended value |
|----------------------------|--|------------------------------|
| Local image base directory | The name of the directory on the installation server containing the IBM Intelligent Operations Center installation files. This is the directory where the installation media files were copied before running the installation tool. This directory is referred to as <code>install_media</code> in other installation instructions. | <code>/installMedia</code> |
| Local image temp directory | The directory on the installation server used to store temporary files during the installation. | <code>/installMedia</code> |
| Local backup directory | This directory is for internal use only. | <code>/tmp/loc/backup</code> |

Table 9. IBM Intelligent Operations Center installation directories (continued)

| Directory | Description | Recommended value |
|-------------------------|---|--------------------------|
| Remote image directory | The directory on the target servers where the packages to be installed on that server will be copied. | /installMedia/loc/image |
| Remote script directory | The directory on the target servers where the installation scripts to be run on that server will be copied. | /installMedia/loc/script |

Related tasks:

“Copying the installation package to the installation server” on page 23

Copy the IBM Intelligent Operations Center installation package to the installation server before installing the product.

Data server location

The IBM Installation Manager allows the installer to define the connection to the data server during the installation of the IBM Intelligent Operations Center.

The installer can specify the data server connection options shown in Table 10.

Table 10. IBM Intelligent Operations Center Data server connection information

| Option | Description | Recommended value |
|----------------------|---|--|
| Data server hostname | The fully qualified host name for the server. | None. Value is installation dependent. |
| Data server user | The Linux user account to be used during the installation process. | root |
| Data server password | The password for the account specified in Data server user . | None. Value is installation dependent. |

To test the connection to the server, click **Test connection**.

Application server location

The IBM Installation Manager allows the installer to define the connection to the application server during the installation of the IBM Intelligent Operations Center.

The installer can specify the application server connection options shown in Table 11.

Table 11. IBM Intelligent Operations Center application server connection information

| Option | Description | Recommended value |
|-----------------------------|--|--|
| Application server hostname | The fully qualified host name for the server. | None. Value is installation dependent. |
| Application server user | The Linux user account to be used during the installation process. | root |
| Application server password | The password for the account specified in Application server user . | None. Value is installation dependent. |

To test the connection to the server, click **Test connection**.

Event server location

The IBM Installation Manager allows the installer to define the connection to the event server during the installation of the IBM Intelligent Operations Center.

The installer can specify the event server connection options shown in Table 12.

Table 12. IBM Intelligent Operations Center event server connection information

| Option | Description | Recommended value |
|-----------------------|--|--|
| Event server hostname | The fully qualified host name for the server. | None. Value is installation dependent. |
| Event server user | The Linux user account to be used during the installation process. | root |
| Event server password | The password for the account specified in Event server user . | None. Value is installation dependent. |

To test the connection to the server, click **Test connection**.

Management server location

The IBM Installation Manager allows the installer to define the connection to the management server during the installation of the IBM Intelligent Operations Center.

The installer can specify the management server connection options shown in Table 13.

Table 13. IBM Intelligent Operations Center management server connection information

| Option | Description | Recommended value |
|----------------------------|---|--|
| Management server hostname | The fully qualified host name for the server. | None. Value is installation dependent. |
| Management server user | The Linux user account to be used during the installation process. | root |
| Management server password | The password for the account specified in Management server user . | None. Value is installation dependent. |

To test the connection to the server, click **Test connection**.

Cyber hygiene configuration

The IBM Installation Manager allows the installer to specify options required for cyber hygiene during the installation of the IBM Intelligent Operations Center.

The installer can specify the cyber hygiene options shown in Table 14.

Table 14. IBM Intelligent Operations Center cyber hygiene options

| Option | Description | Recommended value |
|---------------------------|--|--|
| GRUB password | The bootloader password for the system. This password will be used for all target servers. | A password specified by the customer and consistent with the customer's organization password policy. |
| Disable remote root login | Defines if remote access is disabled for the root user on all target servers. | <p>A checkbox is displayed with the option selected. The option cannot be cleared. Remote root login must be disabled. The option is displayed so the installer understands that remote root login is disabled.</p> <p>This configuration does not disable log on as root from the console or changing to the root user using the su command when logged onto the server.</p> |

Restarting the installation using Installation Manager

If the installation fails, the installation can be restarted.

About this task

If the installation fails, the installation tool will roll back changes made during the session. If multiple installation components were selected, all selected steps will be rolled back even if some of steps successfully completed.

To restart a failed installation, do the following.

Procedure

1. Click **Applications > IBM Installation Manager > IBM Installation Manager**.
2. If no components were successfully installed, select **new** to restart the installation from the beginning.
3. If one or more component was successfully installed, select **modify** to retain existing installation changes. Select the components or components to be installed.

Note: It is recommended that you use the installer to install components one component at a time. This will limit the roll back of successfully installed components if subsequent component installations fail.

Installing IBM Intelligent Operations Center step-by-step

IBM Intelligent Operations Center can be installed using step-by-step installation steps and scripts.

Preparing the installation package

Before running the installation scripts, the installation package needs to be unpacked and prepared.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Copy the installation package to *install_home*.
2. Extract the installation package.
3. Extract BA_1.5_GUI_Installer_Lite_Launchpad.zip to the *install_home* directory.
4. Change to the *install_home/repository/native* directory.
5. Extract com.ibm.iop.ba.lite_1.5.0.9.zip to the *install_home* directory.
6. Extract com.ibm.iop.cat.lite_1.5.0.9.zip to the *install_home* directory.
7. Extract com.ibm.iop.isp.lite_1.5.0.zip to the *install_home/isp/* directory.
8. Extract com.ibm.iop.cyber.hygiene.install.lite_1.5.0.zip to the *install_home/ch* directory.
9. Run the **cp ../files/com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip [install-home]/ch/install** command.
10. Extract com.ibm.iop.ioc.solution.lite_1.5.0.20120807.1518.zip to the *install_home/ioc/spec* directory.
11. Extract com.ibm.iop.ioc.topology.lite_1.5.0.20120807.1518.zip to the *install_home/ioc/topology* directory.
12. Run the **find install_home -name *.sh -exec chmod +x {} \;** command.
13. Run the **find install_home -name *.sh -exec dos2unix {} \;** command.

Verifying the installation scripts

A command can be run to display documentation on the installer. This also shows that the installation package is operational.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as root or switch to the root account by running the `su -` command.
2. Run the `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` command.
3. Run the `install_home/ioc/bin/ba.sh` command. Installation documentation is displayed.

Customizing the installation properties

The installation properties file and topology properties files provide definitions required by the installation scripts.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

Optional: Edit the `install_home/ioc/resource/custom.properties` file and change the following property values if desired. Any properties values in the file not listed in Table 15 should not be changed.

Table 15. IBM Intelligent Operations Center installation properties

| Property | Description | Default value |
|---|--|---------------------------------------|
| <code>image.basedir.local</code> | The name of the directory on the installation server containing the IBM Intelligent Operations Center installation files. This is the directory where the installation media files were copied before running the installation tool. This directory is referred to as <i>install_media</i> in other installation instructions. | <code>/installMedia</code> |
| <code>image.tempdir.local</code> | The directory on the installation server used to store temporary files during the installation. | <code>/installMedia</code> |
| <code>backup.local</code> | This directory is for internal use only. | <code>/tmp/loc/backup</code> |
| <code>Unix.image.basedir.remote</code> | The directory on the target servers where the packages to be installed on that server will be copied. | <code>/installMedia/loc/image</code> |
| <code>Unix.script.basedir.remote</code> | The directory on the target servers where the installation scripts to be run on that server will be copied. | <code>/installMedia/loc/script</code> |
| <code>connection.timeout</code> | Time (in milliseconds) to wait for a connection to the target servers before failing | 120000 |
| <code>waiting.time</code> | Time (in milliseconds) to wait before retrying a failed connection | 120000 |

Table 15. IBM Intelligent Operations Center installation properties (continued)

| Property | Description | Default value |
|-------------|--|---------------|
| retry.count | Number of times to retry a failed connection before failing the installation | 6 |

If unchanged, the default values will be used.

Related concepts:

“Password information” on page 36

Passwords for various user IDs used in the IBM Intelligent Operations Center solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Intelligent Operations Center should be changed.

Installation topology files

IBM Intelligent Operations Center is installed using a topology file. The topology file is an XML file defining the parameters and values used when IBM Intelligent Operations Center is deployed across servers and defines the sequence used to deploy components.

Editing the topology file with a text editor can introduce errors. For this reason all customer-customizable properties are defined in a topology properties file. A topology template file provides the topology structure.

The **parameterizeTopology** command takes the name/value pairs defined in the topology properties file and the structure provided by the topology template file and creates a valid topology file that is then used during installation.

IBM Intelligent Operations Center provides the following topology files:

| File name | Purpose |
|---|---|
| <i>install_home/ioc/resource/custom.properties</i> | Defines the location of the installation media, working directories, and other properties. This file can be edited to meet the needs of the customer’s environment. |
| <i>install_home/ioc/topology/iop_lite_topo.properties</i> | Defines the customer-customizable properties for the deployment including host names and passwords. This file can be edited to meet the needs of the customer’s environment. |
| <i>install_home/ioc/topology/iop_lite_topo.template.xml</i> | Defines the structure of the topology to be deployed. This file uses the values defined in the properties file. This file should not be edited. |
| <i>install_home/ioc/topology/iop_lite_topo.xml</i> | Defines the topology to be deployed. This file is created by the parameterizeTopology command using the information in the properties and template file. This file should not be edited except when necessary to recover from an installation failure. |
| <i>install_home/ioc/topology/iop_lite_topo.chk</i> | Defines the rules used by the Precheck tool to determine if the servers are properly configured for the installation of IBM Intelligent Operations Center. This file should not be edited. |

Related tasks:

“Installing the Platform Control Tool” on page 46

The Platform Control Tool is used to manage the IBM Intelligent Operations Center server environment. The tool is installed separately from the product.

Topology properties file

The topology properties file defines the customer-customizable properties for the deployment of IBM Intelligent Operations Center. This file must be edited to meet the needs of the customer’s environment. Any properties in the provided topology properties file not documented here should not be changed.

After modifying the topology properties file, save a copy to a secure location. The file contains security-sensitive information, such as user names and passwords for the system, in clear text. If an unauthorized person has access to this file, they will have full access to the system.

The topology properties file can be used after installation in the following ways:

- As a repository of password information if a password is forgotten.
- As a repository for passwords when they are changed in the system. The modified topology properties file can be used to update the passwords used by the Platform Control Tool.
- As a backup of installation information if the system needs to be reinstalled. The topology properties file can be used without having to redefine all the installation parameters.

Related tasks:

“Generating the topology file” on page 39

Before running the installation steps for IBM Intelligent Operations Center, generate a topology file with the parameters required for the installation.

Target server information:

The SERVERS section of the topology properties file defines properties for the target servers.

Table 16 shows the server property values that can be specified in the topology properties file.

Table 16. Target server properties

| Property | Description |
|---------------------|--|
| DB.1.HOST | The host name of the data server |
| DB.1.ACCOUNT.PWD | The root password for the data server |
| DB.1.SSH_PORT | The port number for ssh access to the data server |
| APP.1.HOST | The host name of the application server |
| APP.1.ACCOUNT.PWD | The root password for the application server |
| APP.1.SSH_PORT | The port number for ssh access to the application server |
| EVENT.1.HOST | The host name of the event server |
| EVENT.1.ACCOUNT.PWD | The root password for the event server |
| EVENT.1.SSH_PORT | The port number for ssh access to the event server |
| MGMT.1.HOST | The host name of the management server |
| MGMT.1.ACCOUNT.PWD | The root password for the management server |
| MGMT.1.SSH_PORT | The port number for ssh access to the management server |

Important: Host name values must be fully-qualified host names entered in the case defined. For example, IOC15App.IOC15.com is not the same as ioc15app.ioc15.com.

An ssh port number can be set for each server. However, the configured port numbers will only be used by the Platform Control Tool. Port 22 must be enabled for ssh access on each server. Port 22 is required for ssh access by IBM Intelligent Operations Center during installation.

Directory services information:

The topology properties file defines values used to encrypt user passwords and other sensitive data within the directory.

Encryption is based on two values: LDAP.SEED and LDAP.SALT.

Values must be printable ASCII characters. Printable ASCII characters are characters with code point values from 33 to 126. A blank space cannot be used.

Table 17. Directory services properties

| Property | Description |
|-----------|--|
| LDAP.SEED | A 12 to 1016 character string, consisting of printable ASCII characters, between code points 33 through 126. A cryptographically-strong string should be used. For example, a long string comprised of mixed-case letters, number and special characters without common words or phrases. |
| LDAP.SALT | A 12 character string, consisting of printable ASCII characters, between code points 33 and 126. Important: LDAP.SALT must be exactly 12 characters in length. A value of more or less characters will cause the installation to fail. |

Record the LDAP.SEED and LDAP.SALT values outside of the system. The values will be needed if you need to export or replicate directory entries.

Password information:

Passwords for various user IDs used in the IBM Intelligent Operations Center solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Intelligent Operations Center should be changed.

Passwords can only contain alphanumeric characters (a-z, A-Z, 0-9). Unless otherwise noted, passwords must be 30 characters or less.

Table 18. Password properties

| Property | Associated user name | Description |
|-------------------------|----------------------|-------------------------------|
| LDAP.DB.PWD | dsrdbm01 | LDAP directory database |
| LDAP.ADMIN.DN.PWD | cn=root | LDAP administrator bind |
| LDAP.BIND.DN.PWD | cn=bind | LDAP bind |
| LDAP.PROXY.INSTANCE.PWD | tdsproxy | LDAP proxy instance |
| LDAP.PROXY.ADMIN.DN.PWD | cn=root | LDAP proxy administrator bind |
| LDAP.PROXY.BIND.DN.PWD | cn=bind | LDAP proxy bind |

Table 18. Password properties (continued)

| Property | Associated user name | Description |
|---------------------------|----------------------|---|
| TAM.SECMASTER.PWD | none | Security service master password This user is granted privileges equivalent to the root user on the target servers. Because of the access afforded this user, make sure this password a long value, is different from other passwords, and is kept secure. |
| TAM.WEBSEAL.ADMIN.PWD | sec_master | Security service administrator This user is granted privileges equivalent to the root user on the target servers. Because of the access afforded this user, make sure this password a long value, is different from other passwords, and is kept secure. |
| WBM.DB.USER.PWD | db2ibm | Business activity monitoring service database |
| WODM.DB.USER.PWD | db2wodm | Decision management service database |
| WODM.ADMIN.UID.PWD | resAdmin1 | Decision management service administrator |
| WODM.DEPLOYER.UID.PWD | resDeployer1 | Decision management service rule deployer |
| WODM.MONITOR.UID.PWD | resMonitor1 | Decision management service monitor |
| WODM.DB.DC.USER.PWD | wodmdc | Decision console database |
| WODM.rtsAdmin.UID.PWD | rtsAdmin | Decision console administrator |
| WODM.rtsConfig.UID.PWD | rtsConfig | Decision console configuration |
| WODM.rtsUser.UID.PWD | rtsUser | Decision console user |
| UDDI.DB.USER.PWD | db2uddi | UDDI service database |
| IHS.KEYSTORE.PWD | none | HTTP server keystore |
| WAS.ADMIN.ACCOUNT.PWD | waswebadmin | Application services administrator |
| WAS.LTPA.PWD | none | LTPA token |
| PORTAL.ADMIN.ACCOUNT.PWD | waswebadmin | Administrator for the WebSphere® Application Server console for the WebSphere Portal server |
| PORTAL.ADMIN.UID.PWD | wpsadmin | Administrator for the WebSphere Portal server |
| PORTAL.DB.USER.PWD | db2port1 | WebSphere Portal database |
| OMNIBUS.ADMIN.ACCOUNT.PWD | netcool | Event services administrator |
| IMPACT.WAS.ACCOUNT.PWD | wasadmin | System event services administrator |
| TSRM.WAS.ADMIN.PWD | waswebadmin | Service request manager administrator |
| TSRM.DB.USER.PWD | maximo | Service request manager database |

Table 18. Password properties (continued)

| Property | Associated user name | Description |
|-----------------------|--|---|
| TSRM.ADMIN.USER.PWD | maxadmin | Service request manager administrator |
| TSRM.REG.USER.PWD | maxreg | Service request manager user |
| TSRM.INITADM.USER.PWD | maxintadm | Service request manager integration user |
| MGMT.WAS.ADMIN.PWD | waswebadmin | Application services administrator |
| TEPS.DB.USER.PWD | itmuser | Enterprise portal database |
| TIM.STORE.PWD | none | Identity management store |
| TIM.ADMIN.USER.PWD | waswebadmin | Identity manager administrator |
| DOMINO.USER.PWD | notes | Collaboration user |
| DOMINO.ORG.PWD | IBM | Collaboration organization |
| DOMINO.ADMIN.PWD | notes admin | Collaboration administrator |
| DOMINO.ST.ADMIN.PWD | wpsadmin | Collaboration portal administrator |
| DOMINO.ST.BIND.PWD | wpsbind | Collaboration LDAP bind |
| DEFAULT.PWD.DAS | dausr1, dausr2, dausr3, dausr4, dausr5, dausr6, dausr7, dausr8 | Database services administrative server |
| DEFAULT.PWD.DB2 | db2inst1, db2inst2, db2inst3, db2inst4, db2inst5, db2inst6, db2inst7, db2inst8 | Database services data server |
| DEFAULT.PWD.IHS | ihsadmin | HTTP server |
| DEFAULT.PWD.MQM | mqm | Messaging services user |
| MQM.CONN.USER.PWD | mqmconn | Messaging services connection |
| DEFAULT.PWD.TAI | tauser | Application services security |
| ITM.ADMIN.PWD | sysadmin | System management administrator Restriction: Password must be 15 characters or less. |
| IOP.ADMIN.USER.PWD | ibmadmin | 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 afforded this user, make sure this password a long value, is different from other passwords, and is kept secure. |
| IOP.USER.USER.PWD | ibmuser | System general user |

Related concepts:

Chapter 3, “Securing the solution,” on page 65

Security is important within the IBM Intelligent Operations Center because the solution is central to essential operations. To ensure security, it is important that you are aware of the default settings and that you manage users of the solution to give all users the correct level of access.

Related tasks:

“Customizing the installation properties” on page 33

The installation properties file and topology properties files provide definitions required by the installation scripts.

Related reference:

“Sample users” on page 67

During the deployment of the IBM Intelligent Operations Center, sample users are created.

Creating the topology password

The topology password is used during the installation process to encrypt and access the file defining the solution topology.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as root or switch to the root account by running the **su -** command.
2. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
3. Change to the *install_home/ioc* directory.
4. Run the **bin/ba.sh createSecretKey -p password** command where *password* is the password to be created for the topology. This command creates the *install_home/ioc/resource/ioc.keystore* file. This file contains the key used to encrypt the topology properties file. The *ioc.keystore* file is also encrypted with the password specified in the **createSecretKey** command. To change the password and key for the installation, delete the *install_home/ioc/resource/ioc.keystore* file and then rerun the **createSecretKey** command. Make a note of the password for use in other installation steps.

Related tasks:

“Generating the topology file”

Before running the installation steps for IBM Intelligent Operations Center, generate a topology file with the parameters required for the installation.

Generating the topology file

Before running the installation steps for IBM Intelligent Operations Center, generate a topology file with the parameters required for the installation.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as root or switch to the root account by running the **su -** command.
2. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
3. Go to the *install_home/ioc/topology* directory.
4. Edit the *iop_lite_topo.properties* file making any changes required for your environment.

5. Copy the topology template file into the topology file by running the **cp iop_lite_topo.template.xml iop_lite_topo.xml** command.
6. Change to the *install_home/ioc* directory.
7. Run the **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password** command where *password* is the topology password. The parameters defined in the topology properties file are applied to the topology file.
8. Optional: To encrypt passwords in the topology file, run the **bin/ba.sh encryptTopology -t iop_lite_topo -p password** command where *password* is the topology password.

Important: Only the passwords in the topology file will be encrypted. Passwords in other files, for example the topology properties file, will not be encrypted.

Related concepts:

“Topology properties file” on page 35

The topology properties file defines the customer-customizable properties for the deployment of IBM Intelligent Operations Center. This file must be edited to meet the needs of the customer’s environment. Any properties in the provided topology properties file not documented here should not be changed.

Related tasks:

“Creating the topology password” on page 39

The topology password is used during the installation process to encrypt and access the file defining the solution topology.

Running the Precheck tool

Before uploading installation packages to the target servers, check that the target servers are ready for the installation by running the Precheck tool.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as root or switch to the root account by running the **su -** command.
2. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
3. Change to the *install_home/ioc* directory.
4. Run the **bin/ba.sh precheckTopology -t iop_lite_topo -p password** command where *password* is the topology password. Messages will be displayed for each precheck test on each server. The status of each test will be [Pass] or [Fail]. After all tests are run, a summary of all failed tests will be displayed.
5. If there are any failures, take the appropriate action to fix the problem and rerun the Precheck tool until there are no failures.

Results

If message CHK0101W is issued there is no DNS server configured for the environment, or the DNS server does not have your servers defined. This warning can be ignored if your servers are defined using static IP addressing in the */etc/hosts* file.

Related concepts:

“TCP/IP networking” on page 20

Prior to installing IBM Intelligent Operations Center, TCP/IP networking between the servers must be correctly set-up.

Linux security settings

Linux security settings must be changed to enable the Platform Control Tool.

These settings can be changed by running a series of commands or by using a script.

The script makes the changes indicated by the commands. If the commands do not meet the needs of your installation, or if company processes do not allow security changes to be made using a script, change the settings using individual commands.

Manually tailoring Linux security settings

Required Linux security settings can be made by running a series of commands.

Procedure

1. On the installation server log on as root or run the **su** - command to switch to the root account.
2. Do the following to enable the Platform Control Tool. These steps need to be run for each of the following target servers:
 - Application server
 - Data server
 - Event server
 - Management server
 - a. Run the **visudo** command. The `/etc/sudoers` file will open for editing.
 - b. Type the letter `i` to change to insert mode allowing you to make changes to the file.
 - c. Find the following line:

```
#wheel ALL=(ALL) NOPASSWD: ALL
```

And change the line to:

```
%wheel ALL=(ALL) NOPASSWD: ALL
```
 - d. Add the following line to the end of the file:

```
Defaults:%wheel !requiretty
```
 - e. Press `Esc`. Insert mode is exited.
 - f. Enter `:wq`. The file is saved.
 - g. Run the **exit** command. The system returns to the installation server login.

When completed for all four servers, Linux security allows users in the `wheel` group to use the **sudo** command to run system commands locally or from a remote session.

Related tasks:

“Tailoring Linux security settings with a script”

Required Linux security settings can be made by running a script.

Tailoring Linux security settings with a script

Required Linux security settings can be made by running a script.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Change to the `install_home/ioc` directory.
2. Run the `bin/install-prepare-env.sh -d install_home/ioc -f topology/iop_lite_topo.properties -p password` command where `password` is the topology password.

Related tasks:

“Manually tailoring Linux security settings” on page 41

Required Linux security settings can be made by running a series of commands.

The installTopology command

The `installTopology` command uses the information in the topology file to install IBM Intelligent Operations Center.

Before using the topology file to install IBM Intelligent Operations Center, the `installTopology` command will check that the installation files have been copied to the target servers. If the files have not been copied, the `installTopology` command will copy the required files before proceeding.

Using the topology file as a guide, the `installTopology` command will install each IBM Intelligent Operations Center component and do any required configuration. Messages are displayed during the installation indicating the progress of the installation.

If an error occurs during the `installTopology` command processing, the installation might be able to be restarted after resolving why one or more component installations failed. Failed installations are indicated by the installation status in the topology file.

Note: In a virtual environment is suggested that a snapshot of the environment be made before running the `installTopology` command and after each successful installation.

Installation status

The topology file `Status` attribute indicates the installation status of each component . When the `installTopology` command is run, the action indicated in Table 19 will be taken depending on the status for the component.

Table 19. Installation status and actions

| Value | Status | installTopology Action |
|-----------|--|--|
| New | The component has not been installed. | The status will be changed to Uncertain and the component will be installed. When the component installs successfully, the status is changed to Ready. |
| Ready | The component was successfully installed. | Installation of the component will be skipped when the <code>installTopology</code> command is run again. |
| Uncertain | The component was not successfully installed or the installation is in progress. | The component will be installed. When the component installs successfully, the status is changed to Ready. |

Options for installing IBM Intelligent Operations Center components

The installation of IBM Intelligent Operations Center can take many hours. Because of the time required, IBM Intelligent Operations Center can be installed in one or multiple phases.

In a single phase installation, the installation process runs until all components are installed or there is a failure in the installation. If the installation fails, the installation must be restarted from the beginning.

In a multi-phase installation, the installation process is divided into three separate phases:

uploadTopology

Copies the installation files from the installation server to the target servers.

Phase 1

Installs some of the IBM Intelligent Operations Center components creating a base for the installation of the remaining components.

Phase 2

Installs the remaining IBM Intelligent Operations Center components.

When running in a virtualized environment, a snapshot should be taken after each phase should a restart be required.

The **uploadTopology** phase is run as a separate command. If the installation files have already been copied to the target servers, they will not be copied again.

The phase, or phases, to be run are defined in the topology properties file. The **Status.Phase1** and **Status.Phase2** properties determine if the installation phases will be run when the **installTopology** command is run. If set to New the phase will be run. If set to Ready the phase will be skipped.

Installing IBM Intelligent Operations Center architecture in a single phase

The architecture used with IBM Intelligent Operations Center can be installed in a single phase. If you are installing in a virtualized environment, running the installation in a single phase will not allow you to take snapshots during the installation process.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the **su -** command.
2. Copy the files required for the installation to the target servers and install IBM Intelligent Operations Center.
 - a. Change to the *install_home/ioc* directory.
 - b. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
 - c. Run the **bin/ba.sh installTopology -t iop_lite_topo -p password** command where *password* is the topology password.

The installation files required will be copied to the target servers and IBM Intelligent Operations Center will be installed.

Messages are displayed indicating the installation progress. The messages indicate the status of the installed component. The status will be one of the following:

[OK] Component installed successfully.

[Fail]

Component installation failed.

Results

Installation processing can run as long as 14 hours. The IBM Intelligent Operations Center architecture is successfully installed when all messages complete with an [OK] status.

Installing IBM Intelligent Operations Center architecture in multiple phases

The architecture used with IBM Intelligent Operations Center can be installed in a multiple phases. A multi-phase installation will allow you to resolve installation issues earlier, rather than waiting for the completion of the entire installation process. If you are installing in a virtualized environment, running the installation in a multiple phases will also allow you to take snapshots during the installation process.

About this task

Important: Do not shut down the servers between installation phases. Shutting the servers down between phases has not been tested and can result in unpredictable results.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the `su -` command.
2. Run the `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` command.
3. Copy the installation files to the target servers.
 - a. Change to the `install_home/ioc` directory.
 - b. Run the `bin/ba.sh uploadImage -t iop_lite_topo -threadCount 4 -p password` command where `password` is the topology password. The `-threadCount` parameter specifies the number of threads used when copying the installation files. The value can be changed if needed.

The files required for each target server are copied from the installation server to the target servers. This step can run as long as 2 hours.

Messages are displayed indicating the upload progress. The messages indicate the status of the uploaded component. The status will be one of the following:

[OK] Component uploaded successfully.

[Fail]

Component upload failed.

4. Optional: If installing in a virtualized environment, take a snapshot of all target servers. Shut down the virtual machines before taking the snapshot to save disk space and processing time. After taking the snapshot, restart the virtual machines. The snapshot can be used to restart the installation from this point if errors occur during subsequent installation processing.
5. Prepare for running installation phase 1.
 - a. Using a text editor, edit the topology properties file: `install_home/ioc/topology/iop_lite_topo.properties`.
 - b. Change the status values as shown:

```
Status.Phase1="New"
Status.Phase2="Ready"
```

This will tell the installation program to install the first phase and skip the second phase.
 - c. Change to the `install_home/ioc` directory.
 - d. Run the `cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml` command. The topology template file will be copied to the topology file.
 - e. Run the `bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password` command where `password` is the topology password. The property values defined in the topology properties file will be applied to the topology file.
 - f. Optional: Run the `bin/ba.sh encryptTopology -t iop_lite_topo -p password` command where `password` is your topology password. The passwords in the topology file will be encrypted using the supplied topology password.
6. Run installation phase 1.
 - a. Change to the `install_home/ioc` directory.

- b. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
- c. Run the **bin/ba.sh installTopology -t iop_lite_topo -p password** command where *password* is the topology password.

The installation installs base components required for IBM Intelligent Operations Center. This step can run as long as 9 hours.

Messages are displayed indicating the installation progress. The messages indicate the status of the installed component. The status will be one of the following:

[OK] Component installed successfully.

[Fail]

Component installation failed.

7. Optional: If installing in a virtualized environment, take a snapshot of all target servers. Do not shut down the virtual servers before taking the snapshot. When taking the snapshot, include a snapshot of virtual machine memory. The snapshot can be used to restart the installation from this point if errors occur during subsequent installation processing.
8. Prepare for running installation phase 2.
 - a. Using a text editor, edit the topology properties file: *install_home/ioc/topology/iop_lite_topo.properties*.
 - b. Change the status values as shown:


```
Status.Phase1="Ready"
Status.Phase2="New"
```

This will tell the installation program to install the second phase and skip the first phase.
 - c. Change to the *install_home/ioc* directory.
 - d. Run the **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml** command. The topology template file will be copied to the topology file.
 - e. Run the **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password** command where *password* is the topology password. The property values defined in the topology properties file will be applied to the topology file.
 - f. Optional: Run the **bin/ba.sh encryptTopology -t iop_lite_topo -p password** command where *password* is your topology password. The passwords in the topology file will be encrypted using the supplied topology password.
9. Run installation phase 2.
 - a. Change to the *install_home/ioc* directory.
 - b. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
 - c. Run the **bin/ba.sh installTopology -t iop_lite_topo -p password** command where *password* is the topology password.

The installation installs the remaining components required for IBM Intelligent Operations Center. This step can run as long as 4 hours.

Messages are displayed indicating the installation progress. The messages indicate the status of the installed component. The status will be one of the following:

[OK] Component installed successfully.

[Fail]

Component installation failed.

Results

The IBM Intelligent Operations Center architecture is successfully installed when all messages complete with an [OK] status.

Restarting the IBM Intelligent Operations Center architecture installation during a step-by-step installation

If the architecture installation fails, the installation can be restarted.

About this task

To restart a failed installation, do the following.

Procedure

1. Edit the topology file to determine which component failed. This will be indicated by `Status="Uncertain"`.
2. Determine and resolve the cause of the error. The installation must gather tool can be used to collect the installation logs for review.
3. Rerun the `installTopology` command. The installation will be reattempted. All components with `Status="New"` and `Status="Uncertain"` will be installed. Components with `Status="Ready"` have been successfully installed and will be skipped.

What to do next

Sometimes a failed component install will not successfully install. In this case you must recreate the environment before the `installTopology` command was run and then restart the installation. For environment with virtualization, snapshots of the environment can be used to quickly revert the system to the state it was in before the `installTopology` command was run.

Related tasks:

“Running the installation must gather tool” on page 283

Log files are generated while IBM Intelligent Operations Center is installed. A tool is available to gather these log files for analysis.

Installing the Platform Control Tool

The Platform Control Tool is used to manage the IBM Intelligent Operations Center server environment. The tool is installed separately from the product.

Before you begin

The IBM Intelligent Operations Center product must be installed before installing the Platform Control Tool.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the `su -` command.
2. Change to the `install_home/isp/mgmt/setup` directory.
3. Run the `./iopmgmt-install.sh -f install_home/ioc/topology/iop_lite_topo.properties -p password` command where *password* is the password you want to use when accessing the tool. Remember this password since you will need it when running the tool. The Platform Control Tool is successfully installed on the management server when all components are shown installed with the [OK] status.

4. Optional: If you are not using the Java provided by IBM Intelligent Operations Center, on the management server edit the `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` and `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh` files. Change the `export JAVA_HOME=` value in each file to the Java JRE location on the server.

What to do next

Verify that the Platform Control Tool has been installed correctly by starting, stopping, and querying services using the Platform Control Tool.

Related concepts:

“Installation topology files” on page 34

IBM Intelligent Operations Center is installed using a topology file. The topology file is an XML file defining the parameters and values used when IBM Intelligent Operations Center is deployed across servers and defines the sequence used to deploy components.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Querying the status of the services” on page 191

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

Installing the System Verification Check tool

The System Verification Check tool is used to verify the operational status of components in IBM Intelligent Operations Center. The tool is installed separately from the product.

Before you begin

The IBM Intelligent Operations Center product must be installed before installing the System Verification Check tool.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the `su -` command.
2. Run the `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` command.
3. Change to the `install_home/cat/bin` directory.
4. Run the `./install-cat-lite.sh -d install_home/cat -f install_home/ioc/topology/iop_lite_topo.properties -p password` command where *password* is the topology password.

Note: The command must be run from the `install_home/cat/bin` directory.

The System Verification Check tool is successfully installed when all components are shown installed with the [OK] status.

5. Restart all IBM Intelligent Operations Center servers.
 - a. Shut down all IBM Intelligent Operations Center servers using the Platform Control Tool.
 - b. Shut down and restart all servers from the operating system.

- c. Start all IBM Intelligent Operations Center servers using the Platform Control Tool.

What to do next

Verify that the System Verification Check tool has been installed correctly by running the System Verification Check tool.

Related tasks:

“How to use the System Verification Check tool” on page 199

The System Verification Check tool is used to determine the operational status of services comprising the IBM Intelligent Operations Center system.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

Installing the IBM Intelligent Operations Center application

Install the IBM Intelligent Operations Center application after the IBM Intelligent Operations Center architecture, including the System Verification Check and Platform Control Tool, is installed.

Before you begin

The IBM Intelligent Operations Center architecture must be installed and all services started.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the **su -** command.
2. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command.
3. Change to the *install_home/ioc* directory.
4. Run the **cp topology/iop_lite_topo.xml topology/iop_lite_topo_phase2.xml** command.
5. Run the **bin/ba.sh installTopology -t ioc_lite_topo -p password** command where *password* is the topology password. The installation installs the IBM Intelligent Operations Center application. This step can run as long as an hour.

Messages are displayed indicating the installation progress. The messages indicate the status of the installed component. The status will be one of the following:

[OK] Component installed successfully.

[Fail]

Component installation failed.

Results

The IBM Intelligent Operations Center application is successfully installed when all messages complete with an [OK] status.

Verifying the installation

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

Procedure

Start all services.

1. Start all IBM Intelligent Operations Center services by running the Platform Control Tool with the **start all** parameter.
 2. Check that all services have started successfully by reviewing the displayed messages.
 3. Run all the tests in the System Verification Check tool.
 4. Check that all tests have run successfully.
- Optionally shut down and restart all services.
5. Stop all IBM Intelligent Operations Center services by running the Platform Control Tool with the **stop all** parameter.
 6. Check that all services have stopped successfully by reviewing the displayed messages.
 7. Shut down the Linux operating system on all servers.
 8. Power-down and power-up all runtime servers or reboot all servers.
 9. Start all IBM Intelligent Operations Center services by running the Platform Control Tool with the **start all** parameter.
 10. Check that all services have started successfully by reviewing the displayed messages.
 11. Run all the tests in the System Verification Check tool.
 12. Check that all tests have run successfully.

What to do next

If any errors are noted, resolve the errors and rerun these steps.

Related concepts:

“About” on page 185

Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“How to use the System Verification Check tool” on page 199

The System Verification Check tool is used to determine the operational status of services comprising the IBM Intelligent Operations Center system.

Post-installation IBM Intelligent Operations Center configuration

After installing the IBM Intelligent Operations Center architecture using Installation Manager or step-by-step, several post-installation configuration steps need to be done to complete the installation.

Important: All post-installation configuration work needs to be done before cyber hygiene is installed.

Related tasks:

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

Configuring collaboration services for IPv6

If your installation uses IPv6 networking, configuration steps are required for collaboration services.




About this task

The IBM Intelligent Operations Center architecture needs to be installed before configuring IPv6 networking for collaboration services.

Procedure

1. Follow the steps in the Lotus Domino® documentation to configure Lotus Domino for IPv6 addressing.
2. Follow the steps in the Lotus Sametime Standard documentation to configure Lotus Sametime Standard for IPv6 addressing.
3. Follow the steps in the WebSphere Portal documentation to configure trust for the Sametime Contact List portlet if you are not using an IPv4 network with an IPv4 address assigned to the event server.

Related information:

-  [Configuring Lotus Domino for IPv6 addressing](#)
-  [Configuring the Sametime Community Server to support IPv6](#)
-  [Configuring trust for the Sametime Contact List portlet](#)

Configuring single sign-on for collaboration services

Import the WebSphere Portal SSO LTPA token into the event server to allow users to access collaboration services without having to reenter their credentials.

About this task

The IBM Intelligent Operations Center architecture needs to be installed before importing the Lightweight Third-Party Authentication (LTPA) token.

This token was created during the installation of the IBM Intelligent Operations Center architecture.

Procedure

1. Install a Lotus Notes® 8.5.x client on a workstation. An existing installation can be used. The workstation must be able to connect to the event server over TCP/IP using the fully-qualified host name.
2. Copy the `/opt/pdweb/etc/stproxy.ltpa` file from the application server to the workstation running Lotus Notes. This is the LTPA token that will be imported into the collaboration service directory.
3. Copy the `/local/notesdata/admin.id` file from the event server to the workstation running Lotus Notes. This is the ID file for the collaboration service administrator. You will use this ID to login to the collaboration services directory.
4. On the workstation, start the Lotus Notes client and log on with the `admin.id` file.
 - a. On the Lotus Notes log on panel, click **User Name**.
 - b. Navigate to the directory where you copied that `admin.id` file and select it.
 - c. Enter the password defined in the topology properties file for the `DOMINO.ADMIN.PWD` property.
 - d. Click **Yes** if a security warning is displayed.
5. Open the `names.nsf` file.
 - a. Click **File > Open > Lotus Notes Application**.
 - b. Enter the fully-qualified host name of the event server in **Look In**.
 - c. Enter `names.nsf` in **File Name**.
 - d. Click **Open**.
6. Navigate to **Web > Web Configurations**.

7. Select Web SSO Configuration for LTPA Token and click **Edit Document**.
8. Click **Keys > Import WebSphere LTPA Keys**. Click **OK** if a warning is received about overwriting existing keys.
9. Enter the path to where the `stproxy.ltpa` file was copied. Click **OK**.
10. Enter the password for the LTPA token. The password is defined in the topology properties file `WAS.LTPA.PWD` property.
11. Click **OK > Save and Close**.
12. Restart the collaboration service using the Platform Control Tool.
 - a. Log on to the management server and open a terminal window.
 - b. Run `su -ibmadmin`.
 - c. Run `/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop st password` where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.
 - d. Run `/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start st password` where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

Setting the session timeout

The session timeout determines the time a user can remain idle before the session is terminated and the user must log in again. The session time out includes administrators logged in through the portal service.

About this task

When IBM Intelligent Operations Center is installed, no session time out is defined. Users will stay logged in until they log out even if the session is idle.

If your organization has security policies requiring that sessions log out after a period of inactivity, use the following steps to define a session timeout for your IBM Intelligent Operations Center system.

Procedure

1. Using a web browser go to `http://application_server:9060/ibm/console` where *application_server* is the host name of the application server.
2. Log on as the `waswebadmin` user with the password defined for `PORTAL.ADMIN.ACCOUNT.PWD` in the topology properties file.
3. Click **Servers > Server Type > WebSphere Application Servers > WebSphere Portal**.
4. Click **Container Settings > Session management > Set Timeout**.
5. Enter the desired timeout value in minutes.
6. Click **OK**.
7. Click **Save**.
8. Click **Servers > Server Type > WebSphere Application Servers > STProxyServer1**.
9. Click **Container Settings > Session management > Set Timeout**.
10. Enter the desired timeout value in minutes.
11. Click **OK**.
12. Click **Save**.
13. Click **Servers > Server Type > WebSphere Application Servers > CongnosX_GW1**.
14. Click **Container Settings > Session management > Set Timeout**.
15. Enter the desired timeout value in minutes.
16. Click **OK**.
17. Click **Save**.
18. Click **Servers > Server Type > WebSphere Application Servers > CongnosX_Disp1**.

19. Click **Container Settings > Session management > Set Timeout**.
20. Enter the desired timeout value in minutes.
21. Click **OK**.
22. Click **Save**.
23. Stop and restart the application server
24. On the application server log on as the `ibmadmin` user with the password defined for `IOP.ADMIN.USER.PWD` in the topology properties file.
25. Run the `sudo su -` command to switch to the root user.
26. Edit the `/opt/pdweb/etc/webseald-default.conf` file with a text editor.
27. In the `SESSION CACHE SETTINGS` section change the `timeout = 0` value to the desired session timeout in seconds. The timeout must be the same as the time set for the portal service. However, the portal value is set in minutes and the session cache setting is specified in seconds. The session cache settings timeout value must be exactly 60 times the value set for the portal service. For example, if the portal value was 30 (minutes), the session caches settings value must be 1800 (seconds).
28. Run the `/usr/bin/pdweb restart` command to restart the security service.

Installing and configuring semantic model services

IBM Intelligent Operations Center provides a semantic model services application and sample model. This service needs to be installed and configured prior to use.

Configuring the Jazz team server

The IBM Intelligent Operations Center semantic model services is installed on a Jazz team server. The Jazz team server needs to be configured before the IBM Intelligent Operations Center semantic model services are installed.

About this task

The IBM Intelligent Operations Center architecture needs to be installed before configuring the Jazz team server.

Procedure

1. In a web browser go to `http://management_host:82/jts/setup` where *management_host* is the fully qualified host name of the management server.
2. Log on with the user ID `iicsystemuser` and password `passw0rd`.
3. Click **Next**.
4. On the Configure Public URI page, provide a **Public URI Root** value in the form `https://management_host:9448/jts` and select I understand that once the Public URI is set, it cannot be modified.. Click **Next**.
5. Click **Test Connection**. A message should be displayed that the configuration test was successful.
6. Click **Next** to save the settings and continue.
7. Configure the database on the Configure Database page.
 - a. Select DB2 for **Database Vendor**.
 - b. Select JDBC for **Connection Type**.
 - c. Enter the DB2 database password defined as the `DEFAULT.PWD.DB2` property in the topology properties file for **JDBC Password**. Ignore the displayed password message.
 - d. For **JDBC Location** enter `//db_host:50005/JTS:user=db2inst5;password={password}`; where *db_host* is the host name of the data server. The `{password}` string must be entered as shown. Do not substitute with a password value.
 - e. Click **Test Connection**. If an error occurs, check and correct any entries. If the entries are correct, make sure the database services are started on the data server using the Platform Control Tool.

- f. After a message is displayed that no Jazz tables are present in the database, click **Create Tables**. Processing will take several minutes to complete.
- g. Click **Next**.
8. On the Enable E-mail Notification page set the value to **Disabled** and click **Next**.
9. The Register Applications page should display "No new applications detected." Click **Next**.
10. Select **LDAP** for the **User Registry Type** in Step 1 on the Setup User Registry page.
11. In Step 2 configure LDAP for the Jazz Team Server registry.
 - a. Enter `ldap://mgmt_host:389` for **LDAP Registry Location** where *mgmt_host* is the fully qualified host name of the management server.
 - b. Enter `OU=USERS,OU=SWG,O=IBM,C=US` for **Base User DN**.
 - c. Enter `userId=uid,name=cn,emailAddress=mail` for **User Property Names Mapping**.
 - d. Enter `OU=GROUPS,OU=SWG,O=IBM,C=US` for **Base Group DN**.
 - e. For **Jazz to LDAP Group Mapping** make sure the value is set to `JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDWAdmins=JazzDWAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests`.
 - f. Enter `cn` for **Group Name Property**.
 - g. Enter `cn` for **Group Member Property**.
12. Click **Test Connection**. If a warning message is displayed, click **show details**. If the warning is about the mail property you can ignore the message.
13. For **Client Access License Type** select **IBM Integrated Information Core - IIC Model Server**.
14. Click **Next**.
15. For **Configure Data Warehouse** select the **I do not wish to configure the data warehouse at this time** checkbox.
16. Click **Finish** on the Summary page.

Results

The Jazz team server is operational.

Installing semantic model services

The semantic model services and a sample application are provided with IBM Intelligent Operations Center.

About this task

Configuration of the Jazz Team Server on the management server is required before using the semantic model services.

Procedure

1. In a web browser go to `http://management_host:82/jts/admin` where *management_host* is the fully-qualified host name of the management server.
2. On the Server Administration page, click **Server > Configuration > Register Applications**.
3. Click **Add** on the Registered Applications page.
4. Add the Model Server application on the Add Application page.
 - a. Enter `Model Server` for **Application Name**.
 - b. Enter `http://management_host:82/modelserver/scr`, where *management_host* is the fully qualified host name of the management server, for **Discovery URL**.
 - c. Enter a value of your choice for **Consumer Secret** This value will be used to provide access to the application. The value should be treated with the same security as a password.
 - d. Enter `iicsystemuser` for **Functional ID**

The **Application Type** will change to Model Server.

5. If there are no errors, click **Finish**.

Verifying semantic model services configuration

A semantic model services sample application is provided with IBM Intelligent Operations Center and can be used to verify the correct installation and configuration of the semantic model services.

Procedure

1. Prepare the sample model files.
 - a. On the installation server find the `iic15_2_stagebuiltdtoserver.xx.jar` file in the `install_media` directory.
 - b. Expand the `iic15_2_stagebuiltdtoserver.xx.jar` file into a directory of your choice. In the rest of these steps this directory is referred to as `model_home`.
2. Install the sample model.
 - a. In a web browser on the server where `model_home` is located, go to `http://mgmt_host:82/iic/console` where `mgmt_host` is the fully-qualified host name of the management server.
 - b. Log on as the `iicssystemuser` user with `passwd` as the password.
 - c. Click **Model Manager > Ontologies > Browse**.
 - d. Navigate to the `install_media/ioc/image/IIC/install/modelServices/post_install/` directory.
 - e. Open the `rsm.owl` file.
 - f. Click **Load**. The file will be loaded.
 - g. Click **Model Manager > Ontologies > Browse**.
 - h. Navigate to the `install_media/ioc/image/IIC/install/modelServices/post_install/` directory.
 - i. Open the `modelServer.owl` file.
 - j. Click **Load**. The file will be loaded.
 - k. Click **Model Manager > Ontologies > Browse**.
 - l. Navigate to the `install_media/ioc/image/IIC/install/ktpRuntimeServices/post_install/` directory.
 - m. Open the `kpi.owl` file.
 - n. Click **Load**. The file will be loaded.
 - o. Click **Model Manager > Load > Browse**
 - p. Navigate to the `install_media/ioc/image/IIC/samples/rdf/rsm/` directory.
 - q. Open the `IBM01DownstreamSampleRDF.xml` file.
 - r. Click **Load**. The file will be loaded.
 - s. Click **Model Manager > Load > Browse**
 - t. Navigate to the `install_media/ioc/image/IIC/samples/rdf/rsm/` directory.
 - u. Open the `IBM01UpstreamSampleRDF.xml` file.
 - v. Click **Load**. The file will be loaded.
 - w. Click **Model Manager > Load > Browse**
 - x. Navigate to the `install_media/ioc/image/IIC/samples/rdf/rsm/` directory.
 - y. Open the `IBM01DownstreamSampleReferenceRDF.xml` file.
 - z. Click **Load**. The file will be loaded.
 - aa. Click **Model Manager > Load > Browse**
 - ab. Navigate to the `install_media/ioc/image/IIC/samples/rdf/rsm/` directory.
 - ac. Open the `IBM01UpstreamSampleReferenceRDF.xml` file.
 - ad. Click **Load**. The file will be loaded.
3. Verify that the sample model is correctly installed.

- a. Click **Model Manager > Query > Query**. A predefined query will run. An XML structure will be displayed with the query results. The top level tag should be `spargl` and have secondary tags `head` and `results`.
 - b. Click **Model Explorer** and make sure you can browse the model.
4. Use the model to verify the installation of model manager.
 - a. In a web browser on the management server, go to `http://mgmt_host:82/iic/ibmoil` where `mgmt_host` is the fully-qualified host name of the management server.
 - b. Click **IBM Oil Company > Variables**. Web service URLs are displayed.

Results

The semantic model services and IBMOil sample model are installed.

Improving semantic model services performance

Configure the semantic model services provided by IBM Intelligent Operations Center to improve performance when running queries against models.

Procedure

1. In a web browser go to `http://management_host:82/iic/console` where `management_host` is the fully-qualified host name of the management server.
2. Add the property values in Table 20 to the **OPCWEBSERVICE** category.

Table 20. OPCWEBSERVICE properties

| Property | Value |
|--|---------|
| <code>cache.browse.timetolive.second</code> | 3600 |
| <code>cache.timetolive.second</code> | 2592000 |
| <code>cache.wait.second.after.create.action</code> | 1 |

3. Update or add the following properties and values in Table 21 in the RSM category.

Table 21. RSM properties

| Property | Value |
|----------------------------|--|
| <code>mvmViewPath.0</code> | <code>http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue</code> |

Table 21. RSM properties (continued)

| Property | Value |
|------------------------|--|
| mvmViewPath.1 | http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIM-generic#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIM-generic#RSM_MeasurementValue |
| mvmDownLevelPreRequest | 3 |
| mvmCacheProperty.0 | cim:RSM_IdentifiedObject.name |
| mvmMaxQueryURI | 500 |
| mvmMaxSparqlEntry | 4000 |

4. Click **Publish**. The new and modified properties will be saved.
5. Restart the semantic model services using the Platform Control Tool.
6. In a web browser go to `http://management_host:82/iic/console` where *management_host* is the fully-qualified host name of the management server.
7. Make any solution or application-specific changes as needed. If changes are required, the changes will be identified in the product or solution documentation.

Configuring the Platform Control Tool

After installing IBM Intelligent Operations Center, if you have installed a Java JRE different from the one provided with IBM Intelligent Operations Center you need to define the JRE location used by the Platform Control Tool.

Procedure

1. On the management server, edit the `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` file.
2. Change `export JAVA_HOME=` to the location of the Java JRE.
3. Save the changes.
4. On the management server, edit the `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh` file.
5. Change `export JAVA_HOME=` to the location of the Java JRE.
6. Save the changes.

Related tasks:

“Installing the Java runtime environment” on page 24

The Java 6 runtime environment must be installed on the installation server before installing IBM Intelligent Operations Center.

Encrypting the Tivoli Service Request Manager administrative password

Use the following procedure to encrypt the Tivoli Service Request Manager administrative password in Tivoli Netcool/Impact.

Procedure

1. Log on to the Tivoli Netcool/Impact administrative console at `http://event_host:9080/nci/main` where `event_host` is the host name of the event server. Log on as the admin user with the netcool password.
2. Click **IOC Project**.
3. In the Policies section, double-click the policy **IOC_Sample_Password_Encoder**. The policy is opened in the Policy Editor window.
4. In the **Enter Password Here** field, enter the password for Maxadmin. The Maxadmin password is the administrative user password that you entered during installation.
5. To save the policy, click **Save**.
6. Click the **Trigger Policy** icon.
7. Click **Execute**.
8. In the Service Status section, scroll to **PolicyLogger**, click **View log for PolicyLogger** (icon with the down arrow).
9. In the policy logger window, locate the statement that is similar to the following statement:

```
11 May 2012 14:19:12,260: [IOC_Sample_Password_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
```
10. Copy the encrypted **Maxadmin** password from the statement, for example:

```
{aes}FF877B74ADF4DF1C2002F94ACB38FAFF
```
11. In the Tivoli Netcool/Impact administrative console, in the Policies section, double-click the policy **UTILS_LIBRARY_IOC_TSRM**. The policy is opened in the Policy Editor window.
12. Replace the value of `MAXAdminPassword` with the encrypted value that you copied in Step 10:

```
MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";
```
13. To save the policy, click **Save**.
14. Click **IOC Project**.
15. In the Policies section, double-click the policy **IOC_Sample_Password_Encoder**. The policy is opened in the Policy Editor window.
16. In the **Enter Password Here** field, delete the password for **Maxadmin**.
17. To save the policy, click **Save**.

Setting the minimum number of threads for the EventProcessor

The minimum number of threads for the EventProcessor needs to be set to 25 for performance reasons.

Procedure

1. Log on to the Tivoli Netcool/Impact administrative console at `http://event_host:9080/nci/main` where `event_host` is the host name of the event server.
2. Click **Service Status > EventProcessor**.
3. Specify 25 for **Minimum Number of Threads**.

Note: The **Minimum Number of Threads** value cannot be greater than the value for **Maximum Number of Threads**.

4. Click **OK**.
5. Click the stop process icon to stop the EventProcessor.
6. Click the start process icon to start the EventProcessor.

Changing the Default and WebContainer thread pool size

The Default and WebContainer thread pool size settings need to be changed to improve performance of standard operating procedures.

Procedure

1. On the event server in the WebSphere Portal Administration Interface click **Intelligent Operations > Administration Tools > Administration Consoles**.
2. Under Event Server, click **Standard Operating Procedure Application Server**.
3. Log on as the WebSphere Application Server administrator. The user ID was defined in the WAS.ADMIN.ACCOUNT property and password was defined in the WAS.ADMIN.ACCOUNT.PWD property in the Topology Properties file when the IBM Intelligent Operations Center was installed.
4. Click **Servers > Application servers > MXServer1 > Thread Pools > WebContainer**.
5. Enter 50 for **Minimum Size**.
6. Enter 50 for **Maximum Size**.
7. Click **OK**.
8. Click **Servers > Application servers > MXServer1 > Thread Pools > Default**.
9. Enter 20 for **Minimum Size**.
10. Enter 50 for **Maximum Size**.
11. Click **OK**.
12. Restart the TSRMCluster.
 - a. Click **Servers > Clusters**.
 - b. Select TSRMCluster.
 - c. Click **Stop**.
 - d. Wait for the status to change to red.
 - e. Click **Start**.

Installing and running cyber hygiene step-by-step

Cyber hygiene is installed and run separately from IBM Intelligent Operations Center and must be installed and run after all other IBM Intelligent Operations Center components are installed, configured, and are operational. Cyber hygiene changes the default operating system configuration to a more secure set of options that help to assure a more secure foundation for the IBM Intelligent Operations Center system.

Before you begin

Note: Cyber hygiene is installed and run in the same step. If you are installing IBM Intelligent Operations Center using IBM Installation Manager, do not use these steps. The IBM Installation Manager installation provides an option to install and run cyber hygiene.

To reduce the time cyber hygiene runs scans and remediation, unmount any file system not required to be assessed for security. For example, the *install_media* directories on each server can be deleted after all installation steps are complete. These directories can be deleted or unmounted before running cyber hygiene.

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

About this task

Cyber hygiene should be the last step after installation of the IBM Intelligent Operations Center. The scan and remediations address configuration security exposures that exist after default operating system and the IBM Intelligent Operations Center product are installed. The remediations applied have been tested to confirm that IBM Intelligent Operations Center services will operate correctly.

Changes applied to the system by cyber hygiene can cause problem with other applications and solutions. For example, other applications and solutions might have requirements on the Linux environment that are not in accord with good security practices. An application or solution might require for the system to be logged on as the root user to be installed or run. In this case some of the cyber hygiene changes might need to be temporarily or permanently changed or another solution found from the supplier of the application or solution.

Once cyber hygiene changes are made, there is no automated method to change them. Any changes must be made by manual updates to the Linux operating system or by changing file or directory permissions.

Procedure

1. On the installation server open a terminal window and log on as root. If not logged on as root, switch to the root account by running the **su -** command.
2. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command. The JAVA_HOME variable is set to the Java runtime environment (JRE).
3. Change to the *install_home/ch/install* directory.
4. Edit the *iop-ch-install.xml* file using a text editor.
5. Replace the parameters in the *iop-ch-install.xml* file with the values appropriate for you installation.

Table 22. Cyber hygiene installation parameters

| Parameter | Value |
|-----------------------------------|--|
| <code>\${APP.1.HOST}</code> | The fully-qualified host name of the application server |
| <code>\${APP.1.ACCT}</code> | The Linux user name for SSH access to the application server |
| <code>\${APP.1.ACCT.PWD}</code> | The password for <code>\${APP.1.ACCT}</code> |
| <code>\${APP.1.SSH_PORT}</code> | The application server SSH port |
| <code>\${DB.1.HOST}</code> | The fully-qualified host name of the data server |
| <code>\${DB.1.ACCT}</code> | The Linux user name for SSH access to the data server |
| <code>\${DB.1.ACCT.PWD}</code> | The password for <code>\${DB.1.ACCT}</code> |
| <code>\${DB.1.SSH_PORT}</code> | The data server SSH port |
| <code>\${EVENT.1.HOST}</code> | The fully-qualified host name of the event server |
| <code>\${EVENT.1.ACCT}</code> | The Linux user name for SSH access to the event server |
| <code>\${EVENT.1.ACCT.PWD}</code> | The password for <code>\${EVENT.1.ACCT}</code> |
| <code>\${EVENT.1.SSH_PORT}</code> | The event server SSH port |
| <code>\${MGMT.1.HOST}</code> | The fully-qualified host name of the management server |
| <code>\${MGMT.1.ACCT}</code> | The Linux user name for SSH access to the management server |
| <code>\${MGMT.1.ACCT.PWD}</code> | The password for <code>\${MGMT.1.ACCT}</code> |
| <code>\${MGMT.1.SSH_PORT}</code> | The management server SSH port |

6. Save the file.
7. Change to the *install_home/ch* directory.
8. Run the ***install_home/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d install_media/ioc/image -p GRUB_password*** command where *GRUB_password* is the password to the GRUB bootloader on the servers. The *GRUB_password* will be applied to all target servers. Normally when servers are restarted,

no password is required. However, once cyber hygiene is installed, if you start a server with any Linux option, such as starting in single-user mode, the `GRUB_password` will have to be entered on the server console.

Results

The processing time is determined by the speed of the hardware and if extra, unnecessary files are on the target servers. Processing can run up to 1.5 hours. During that time target servers will be scanned and the appropriate remediation applied.

What to do next

Check the cyber hygiene log for any error. The logs will also show the applied remediations and optional manual steps.

Related concepts:

“Cyber hygiene overview” on page 76

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Changes to the Linux operating system

Cyber hygiene scans the Linux operating system for well-known security exposures and makes appropriate changes. Logs describe the scanned exposures and the changes made to Linux OS policies and settings.

The logs also list exposures that were detected, but where no changes were made. These can include:

- The system is already configured the way cyber hygiene would have changed it.
- The change requires that a system administrator take action or decide if the change is appropriate to the environment.
- The change cannot be made by an automated script. For example, the exposure relates to the general security policies of the organization.

Any remediation applied by cyber hygiene can be changed later if needed. The cyber hygiene logs provide information on the changes applies to the system. Changes might be required to use the system with other applications or solutions if changes made by cyber hygiene are incompatible with those systems.

Reviewing the cyber hygiene log

After cyber hygiene is installed and run, review the log to understand the changes that were made to the system and any remaining exposures.

About this task

On the installation server, go to the directory where the IBM Intelligent Operations Center installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Review the cyber hygiene log in the `/var/ibm/InstallationManager/logs/native` directory on the installation server for completeness ensuring all actions were run on all servers. The log can be found by running the `fgrep yber *.log` command. The log file will show information for each server. In general the steps with log information include:
 - Preparing the environment to run the cyber hygiene tasks.
 - Running the stand-alone remediator. This fixes exposures that do not require scanning. For example, setting a GRUB bootloader password and turning on auditing.

- Disabling remote root log on.
 - Scanning for exposures. These are run in the background and the main tasks waits for scanning to complete.
 - Running the remediator to address exposures found during the scan.
 - Scanning after remediation. This identifies exposures not found during the initial scan.
 - Running the remediator to address additional exposures found during the second scan. Remediations not completed are logged.
2. Review the detailed cyber hygiene logs located in the `/var/BA15/CH/results` directory on each of the target servers. The `standrem-date_time.log` shows the stand-alone remediator results. The `standrem-disableRemoteRoot-date_time.log` shows the results of disabling the remote root log on. The `scanrem-combined-log-date_time.log` shows the results of the scanned remediator actions. There are two logs for the two scan/remediation steps.
 - a. Review the log files for lines starting with the text `Vulnerability`. Each line indicates the action taken and includes:
 - The findings from the scan.
 - The selected remediations.
 - The details on the applied remediations.
 - b. In the log for the second scan and remediation, remediations noted with the text `NOT DONE` might need to be investigated for additional manual actions.

Re-enabling remote root log on

Cyber hygiene disables remote log on to the root account through the `ssh` command. The `telnet` and `rsh` commands are completely disabled in the Linux operating system. If needed, remote log on can be re-enabled.

About this task

Re-enabling remote log on for the root user might not be required. A user with the appropriate privileges can use the `su` and `sudo` commands to operate as the root user. Privileged users operating as the root user are logged for audit purposes.

IBM Intelligent Operations Center defines the `ibmadmin` user in the `wheel` group. Users in the `wheel` group can use the `sudo su -` command to run as root.

Procedure

Do the following to enable root log on using the `ssh` command.

1. Edit the `/etc/ssh/sshd_config` file on the server where remote login as root using `ssh` or a remote terminal is required.
 2. Change the `PermitRootLogin` parameter to `yes` and save the file. Change this parameter to `no` if remote login using the `ssh` command needs to be disabled.
 3. Save the file.
 4. Restart the `ssh` service by running the `service sshd restart` command.
- Remote log on to the root account using remote terminals is disabled by cyber hygiene. Only the screen and keyboard physically connected to the server can log on as the root user. Do the following to re-enable remote root log on to a server from a remote terminal.
5. Edit the `/etc/securetty` file on the server where remote log on as root using `ssh` or a remote terminal is required.
 6. Add the Linux device names for the terminals authorized to log on remotely as the root user. For example, if you want to add `tty1`, change the list to read:

```
console
tty1
```

To disable a terminal, place a # character before the terminal to be disabled. For example:

```
console
#tty1
```

7. Save the file.

Configuring users requiring ssh access

IBM Intelligent Operations Center requires certain users to be configured with ssh access and passwords.

About this task

The following users must be configured on the installation server and all target servers to have ssh access and passwords.

- ibmadmin
- ibmuser
- mqconn

Installing tools provided with the solution

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

With the exception of Rational® Application Developer, these are provided on the IBM Intelligent Operations Center Developer's Toolkit DVD or image. Rational Application Developer is included with the IBM Intelligent Operations Center on separate DVDs or images.

Lotus Sametime Client

For information on installing and using the Lotus Sametime Client , see the Lotus Domino and Lotus Notes information center.

WebSphere Message Broker Toolkit

For information on installing and using the WebSphere Message Broker Toolkit, see the WebSphere Message Broker information center.

IBM WebSphere Business Monitor Development Toolkit

For information on installing and using the IBM WebSphere Business Monitor Development Toolkit, see the IBM WebSphere Business Monitor information center.

Rational Application Developer





For information on installing and using Rational Application Developer, see the Rational Application Developer information center.

Related concepts:

“Creating and integrating KPIs” on page 105

Key performance indicator (KPI) models can be created and modified using a business monitoring development toolkit and a KPI management portlet.

Related information:

-  Lotus Domino and Lotus Notes information center
-  WebSphere Message Broker information center
-  IBM Business Monitor information center
-  Rational Application Developer information center

Deleting sample users

The IBM Intelligent Operations Center is shipped with sample users. For security reasons these users should be deleted after the IBM Intelligent Operations Center is installed in a production environment.

About this task

To delete the predefined users, complete the following steps:

Procedure

1. On the application server, sign into WebSphere Portal.
2. On the **Administration** portal, click **Access > Users and Groups > All Authenticated Portal Users**.
3. Click the delete icon for the following users:
 - tdelorne
 - scollins
 - akelly

Important: Do not delete the following required users. If you delete them, IBM Intelligent Operations Center will not operate properly.

- admin
- iicsystemuser
- maxadmin
- maxintadm
- maxreg
- notesadmin
- resAdmin1
- resDeployer1
- resMonitor1
- rtsAdmin
- rtsConfig
- rtsUser
- taiuser
- SRMSELFSERVICEUSR
- wasadmin
- waswebadmin
- wpsadmin

- wpsbind
- All user IDs beginning with "PM"

Related reference:

“Sample users” on page 67

During the deployment of the IBM Intelligent Operations Center, sample users are created.

Removing installation services from the production system

After installing IBM Intelligent Operations Center, the installation services can be removed from the production system servers. It is suggested that the installation server be kept since some of its services might be required for maintenance activities.

After the installation has completed and the installation has been verified, components that are only used in the installation process can be removed from the production system servers (application server, event server, management server, data server). These include:

- The directory defined by the `Unix.image.basedir.remote` property in the topology properties file.
- The directory defined by the `Unix.script.basedir.remote` property in the topology properties file.
- The `install_media` directory, defined by the `image.basedir.local` property in the topology properties file.

Note: The installation server should be kept if required for future use. Since the topology properties file contains passwords in clear text, this server should be in a secure location.

Related tasks:

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

Chapter 3. Securing the solution

Security is important within the IBM Intelligent Operations Center because the solution is central to essential operations. To ensure security, it is important that you are aware of the default settings and that you manage users of the solution to give all users the correct level of access.

Default passwords

Your first task in securing the solution is to ensure that all default passwords are changed. For more information about the default passwords, see the link at the end of the topic.

Secure connection

The IBM Intelligent Operations Center is HTTPS enabled by default. You can change HTTPS settings for the following individual services within the IBM Intelligent Operations Center:

- The business monitoring service which processes KPIs
- The resource and standard operating procedure administration service

Any change to the HTTPS setting for an individual service must be accompanied by an update to the corresponding port setting. For more detail on changing these settings in the system properties table, see the link at the end of the topic

User authentication

User authentication is associated with authorization rights that give the user access to the appropriate features and data. The IBM Intelligent Operations Center supports integration to the existing security infrastructure for single sign-on.

IBM Intelligent Operations Center user permissions are managed through WebSphere Portal users and groups. WebSphere Portal uses the Lightweight Directory Access Protocol (LDAP) database provided by the Tivoli Directory Server running on the data server.

The security system provided with the IBM Intelligent Operations Center can accommodate many user groups, roles, and permissions. Accommodating many user groups, roles, and permissions can lead to a security regime that is difficult to manage. It is recommended that administrators restrict the number of groups and permissions.

User roles and permissions

Membership of a role-based user group provides a way of controlling access to the IBM Intelligent Operations Center. The users in a group have access only to the features of the solution corresponding to their role. Being a member of a role-based user group also helps users to focus on the appropriate tasks. The standard roles are: Executive, Supervisor, and Operator.

To add a user to the IBM Intelligent Operations Center:

1. Choose a group appropriate to the role of the user in the organization and make the user a member of that group.
2. Complete a profile for the user and include at least the user ID, name, and password.

Data categories and permissions

The security of data that is stored in databases in the IBM Intelligent Operations Center is managed by implementing role-based access to the databases. Access to a feature of the IBM Intelligent Operations Center does not mean that all data is available to the user. Data security is applied at the server level to ensure that users see only the appropriate data. The standard categories are: Geophysical, Transportation, Meteorological, Environmental, Infrastructure, Chemical, Biological, Safety, Security, Rescue, Fire, Health, and Other.

Portal

The portal service provides a platform that can be scaled to accommodate the required set of users. It also provides role-based access that can be adjusted to reflect the required organization structure. You can view, create, and delete users or user groups with the **Manage Users and Groups** portlet. You can also change group memberships. For more information about this portlet, see the link at the end of this topic.

Related concepts:

“Password information” on page 36

Passwords for various user IDs used in the IBM Intelligent Operations Center solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Intelligent Operations Center should be changed.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

User roles and access

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

To use a specific feature of the IBM Intelligent Operations Center, a user must be a member of the user role group that provides the required access to that feature. A user is made a member of a user role group by an administrator. The following table shows how real-life roles might map to the user role groups with login access levels in the IBM Intelligent Operations Center.

Table 23. Job roles and IBM Intelligent Operations Center user role groups

| Job Role | Responsibilities | User role group |
|-----------------------|---|----------------------|
| Executive | <ul style="list-style-type: none">• Defines event, incident, and key performance indicator (KPI) input requirements and thresholds• Views high level visual summaries, details, and reports of:<ul style="list-style-type: none">– KPIs– Events• Communicates policy, long-term direction, or high-level decisions | City-wide Executive |
| Supervisor or manager | <ul style="list-style-type: none">• Manages events and incidents• Produces and monitors KPI reports• Issues alerts• Analyzes events for change of status or action requirements• Decides on short-term corrective measures | City-wide Supervisor |

Table 23. Job roles and IBM Intelligent Operations Center user role groups (continued)

| Job Role | Responsibilities | User role group |
|--------------------|--|--------------------|
| Operator | <ul style="list-style-type: none"> • Monitors event information • Monitors alerts • Views details • Issues communications • Updates event or incident data with further information, for example: <ul style="list-style-type: none"> – Telephone reports – Inputs from construction or maintenance | City-wide Operator |
| User Administrator | Administers all aspects of users including defining groups, assigning permissions to groups, and assigning users to groups. Provides users with the correct access level. Access level is assigned based on group membership. | wpsadmins |

Before customizing roles and defining users for your organization, familiarize yourself with the IBM Intelligent Operations Center security system.

Related tasks:

“Adding a user or group” on page 71

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

Related reference:

“User role groups and authorization permissions” on page 68

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 70

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

Sample users

During the deployment of the IBM Intelligent Operations Center, sample users are created.

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 the following table. Other users are required for administration of the solution.

Table 24. Users defined in the IBM Intelligent Operations Center

| User ID | User role group |
|----------------------|----------------------|
| Sample users | |
| tdelorne | City-wide Executive |
| scollins | City-wide Supervisor |
| akelly | City-wide Operator |
| Required user | |
| wpsadmin | wpsadmins |

When you are ready to define users for your organization, delete the sample users only. You must not delete the wpsadmin user. The wpsadmin user is essential for administration tasks associated with the IBM Intelligent Operations Center. For more information about required users, see the link at the end of this topic.

Important: Replace the default password of the wpsadmin user with a new password. For information about updating portal administrator user IDs and passwords, see the WebSphere Portal documentation.

Related concepts:

“Password information” on page 36

Passwords for various user IDs used in the IBM Intelligent Operations Center solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Intelligent Operations Center should be changed.

Related tasks:

“Deleting sample users” on page 63

The IBM Intelligent Operations Center is shipped with sample users. For security reasons these users should be deleted after the IBM Intelligent Operations Center is installed in a production environment.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

User role groups and authorization permissions

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

An administrator assigns a role to a user by making the user a member of the corresponding user role group. Each user is assigned membership of one or more user role groups.

The following table lists the permissions for each user role group supplied with the IBM Intelligent Operations Center. For each user role group, an authorization permission is granted for each feature in the IBM Intelligent Operations Center.

Table 25. IBM Intelligent Operations Center features and associated user role group permissions

| Feature type | Feature name | City-wide Executive | City-wide Supervisor | City-wide Operator | wpsadmins |
|--------------|------------------------|---------------------|----------------------|--------------------|--------------------------|
| Page | Supervisor: Status | User permission | User permission | None | Administrator permission |
| | Supervisor: Operations | User permission | None | 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 |

Table 25. IBM Intelligent Operations Center features and associated user role group permissions (continued)

| | | | | | |
|---------|---------------------------------------|-----------------|-----------------|-----------------|--------------------------|
| 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 IBM Intelligent Operations Center authorization permissions are assigned based on Lightweight Directory Access Protocol (LDAP) groups. The permissions are defined as follows:

- User permission is the authority granted to a user to give them access to view and work with features.
- Administrator permission is the authority granted to an administrator to give them access to:
 - Configure features
 - Create, modify or delete users and user groups

To access data in IBM Intelligent Operations Center a user must be a member of the user category group that provides the required data permissions.

Related concepts:

“User Permissions Summary” on page 76

Use the User Permissions Summary portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

“User roles and access” on page 66

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

Related tasks:

“Adding a user or group” on page 71

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

“Viewing or modifying group membership” on page 72

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

Related reference:

“User category groups and data permissions”

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

Related information:

 IBM WebSphere Portal 7 Product Documentation

User category groups and data permissions

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

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 of one or more user category groups.

The following table lists the data categories covered by the IBM Intelligent Operations Center and the corresponding user category groups used to identify event, key performance indicator (KPIs), and alert data. For example, if a user wants to be able to see events related to the city’s water department, the user must be a member of the group `ioc_base_infrastructure`.

Table 26. User category group descriptions and identifiers

| Data category | Description | User category group |
|---------------|---|--|
| CBRNE | Chemical, biological, radiological, nuclear, or high-yield explosive threat or attack | <code>ioc_base_chemical</code> , <code>ioc_base_biological</code> , <code>ioc_base_radiological</code> , <code>ioc_base_nuclear</code> , <code>ioc_base_explosive</code> |
| Env | Environment: pollution and other environmental | <code>ioc_base_environmental</code> |
| Fire | Fire suppression and rescue | <code>ioc_base_fire</code> |
| Geo | Geophysical (including landslide) | <code>ioc_base_geophysical</code> |
| Health | Medical and public health | <code>ioc_base_health</code> |
| Infra | Infrastructure: utility, telecommunication, other non-transport infrastructure | <code>ioc_base_infrastructure</code> |
| Met | Meteorological (including flood) | <code>ioc_base_meteorological</code> |
| Rescue | Rescue and recovery | <code>ioc_base_rescue</code> |
| Safety | General emergency and public safety | <code>ioc_base_safety</code> |

Table 26. User category group descriptions and identifiers (continued)

| Data category | Description | User category group |
|---------------|---|-------------------------|
| Security | Law enforcement, military, homeland, and local/private security | ioc_base_security |
| Transport | Public and private transportation | ioc_base_transportation |
| Other | Other events, KPIs, or alerts | ioc_base_other |

To login and access features of the IBM Intelligent Operations Center, a user must be a member of the user role group that provides the required authorization permissions.

Related concepts:

“User Permissions Summary” on page 76

Use the User Permissions Summary portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

“User roles and access” on page 66

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

Related tasks:

“Adding a user or group”

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

“Viewing or modifying group membership” on page 72

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

Related reference:

“User role groups and authorization permissions” on page 68

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Adding a user or group

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

About this task

First select a user role group to set the correct level of access permissions when adding a new user. Then complete the fields on the **Profile Management** page so that the IBM Intelligent Operations Center has the required information to add the new user. Follow the link at the end of the topic for more information about what you can enter in the fields on the **Profile Management** page.

Procedure

1. Log on to <http://app-host/wpsv70/wps/myportal/> as an administrative user.
2. Click **Administration** on the navigation bar at the top of the page.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** on the submenu.
5. If you are adding a new user, select a role by giving the user membership of a group. Search for the group by clicking **All Portal User Groups** for a list of groups and click the required group.

6. Click **New User** or **New Group**.
7. If you are creating a user group, enter a name for the user group.
8. If you are adding a new user, ensure that you enter all of the required fields in the user profile as indicated by the asterisks.
9. Click **OK** to submit the new profile or group.

Results

A message confirms if the submission is successful. A new user profile is created and displayed on the group list or a new group is displayed. The new user is authorized to access the IBM Intelligent Operations Center according to the permissions assigned to the role group selected.

What to do next

- Give the new user membership of data category groups according to the data permissions required.
- If a new group has been added, add the group to the WebSphere Application Server Network Deployment junction ACL.
- If a new group has been added, authorization permissions must also be set for the group. The authorization permissions define what features and data members of the group can see and modify. For information on setting authorization permissions, see the IBM WebSphere Portal 7 Product Documentation link at the end of topic and search for information on assigning access to pages.
- Assign the new user to a security group and person group in Tivoli Service Request Manager.

Note: To save time you can duplicate group assignments for a new user based on an existing user. Select the new user and click the **Duplicate** icon. Select the existing user to duplicate group membership.

Related concepts:

“User roles and access” on page 66

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

Related tasks:

“Configuring new users in Tivoli Service Request Manager” on page 121

When you add a user in IBM Intelligent Operations Center, assign permissions and person groups for the user in Tivoli Service Request Manager.

Related reference:

“User role groups and authorization permissions” on page 68

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 70

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Viewing or modifying group membership

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

About this task

Select the group corresponding to the role or data category for which you want to view or change membership. Membership of a role group gives users access to the parts of the solution appropriate to that role. Membership of a category group gives users access to the events, key performance indicators (KPIs), and alerts associated with that category.

Hover over an icon to view hover help indicating the purpose of the icon.

Procedure

1. Log on to `http://app-host/wpsv70/wps/myportal/` as an administrative user.
2. Click **Administration** on the navigation bar at the top of the page.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** from the submenu.
5. Click **All Portal User Groups** for a list of groups and click the group you require. The members of the group are listed.
6. You can perform the following actions in relation to group membership:
 - View membership of other groups by clicking **View membership** for the user ID.
 - Add a user or users to the group by clicking **Add member** and selecting the user or users to be added.
 - Remove a user from the group by clicking **Remove** for the user ID.

Related reference:

“User role groups and authorization permissions” on page 68

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 70

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Viewing or editing a user profile

View or edit the profile of a user to set or reset any of the user profile attributes including password. You cannot change the user ID.

About this task

Select the user from the authenticated portal users list to open the user profile and change profile details. Each user can also change their own profile.

Hover over an icon to view hover help indicating the purpose of the icon.

Procedure

1. Log on to `http://app-host/wpsv70/wps/myportal/` as an administrative user.
2. Click **Administration** from the top navigation bar.
3. Click **Access** item on the sidebar menu.
4. Click **Users and Groups** from the submenu.
5. Click **All Authenticated Portal Users** for a list of users.

6. Click the edit icon for the user to display the **Profile Management** page. The attribute fields for the user profile are displayed.
7. If you want to change the password, enter a new password in the **New Password:** and **Confirm Password:** fields.
8. You can enter, edit, or delete information in any of the remaining fields.
9. Click **OK** to submit the changes you have made.

Results

The user profile is updated with the changes you submitted.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Deleting a user or group

Delete a user or group from the IBM Intelligent Operations Center.

About this task

To delete a user, select the user from the list of authenticated portal users and delete. To delete a group, select the group from the list of portal user groups and delete.

Hover over an icon to view hover help indicating the purpose of the icon.

Note: Be aware that deleting a user from the IBM Intelligent Operations Center also removes their access to other solutions within the IBM Smarter Cities™ Software Solutions product family. Deleting a group also removes that group from other solutions.

Procedure

1. Log on to `http://app-host/wpsv70/wps/myportal/` as an administrative user.
2. Click **Administration** on the top navigation bar.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** on the submenu:
 - Click **All Portal User Groups** to display a list of groups.
 - Click **All Authenticated Portal Users** to display a list of users.
5. Click the **Delete** icon corresponding to the user or group that you want to delete.

Results

The user or group that you delete no longer exists in the IBM Intelligent Operations Center. Deleting a group does not delete members of the group.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Importing users and groups

You can import users in bulk into the IBM Intelligent Operations Center through the portal service.

About this task

As a portal administrator, you can import users in bulk into the IBM Intelligent Operations Center through the portal administration console. The XML file required for this task can be found on the application server: `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml`. This XML file can be modified to add users to the IBM Intelligent Operations Center.

Note: When adding multiple users, add all the users first, before adding the users to groups. See the example at the end of the topic.

As an alternative to following procedure, you can run from the command line the `xmlaccess.sh` script which is located on the application server.

Procedure

1. Update the `CreateUser.xml` file to contain new users and the groups to which they belong.
2. Log on to `http://app-host/wpsv70/wps/myportal/` as an administrative user.
3. Click **Administration**.
4. Under **Portal Settings**, click **Import XML**.
5. Browse to locate your updated XML file.
6. Click **Import**.

Results

The WebSphere Portal Server automatically creates the associated entries in the directory on the Tivoli Directory Server and in Tivoli Access Manager WebSEAL.

Example

The following example modifies the XML file to add two users to the IBM Intelligent Operations Center and to add each to one role group and one category group:

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true"
portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
```

```
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```

Related concepts:

“Administration Consoles” on page 192

Use the Administration Consoles portlet to administer the services provided by the solution.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

 [Tivoli Directory Server Information Center](#)

 [Tivoli Access Manager Information Center](#)

User Permissions Summary

Use the User Permissions Summary portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

The User Permissions Summary portlet displays details of group membership and permissions granted to users.

To access the User Permissions Summary portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Administration Tools > User Permissions Summary**.

Use the **User** tab to check permissions for a user. Enter the user ID to view the following information:

- 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 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 indicates whether the specified user has permission for that category.

Use the **Summary** tab to check summary statistics for users and group permissions. You can view the following information:

- Total number of groups in the IBM Intelligent Operations Center.
- Total number of users 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.

Related reference:

“User role groups and authorization permissions” on page 68

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 70

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

Cyber hygiene overview

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Note: Commonly, the term "vulnerability" is used to refer to both security vulnerabilities and security exposures. Cyber hygiene defines a vulnerability as a programming error in an application that enables security breaches. Cyber hygiene defines an exposure as an operating system or application configuration selection that is less secure. Exposures can be addressed by choosing a more secure configuration option. For example, a directory can be configured to allow all users to store files there. It can also be configured more securely so that only the owner can store files in the directory.

Cyber hygiene has two key elements:

- Mitigation and correction of known security exposures in the Linux operating system and its associated users, directories, and files. It does this through a set of tools and scripts.
- Documentation of the assessment of almost 1000 known vulnerabilities and exposures in the operating system, products, and system configuration.

By handling security exposures during the installation process, less work is required by the customer to achieve an increased security level in the deployed system.

For example, a government agency can use the cyber hygiene remediation and documentation to help support certification and accreditation of the system for deployment on a secure network. Commercial business customers can use the same process to improve the security of their environment.

Cyber security provides risk mitigation, not risk prevention. Since systems must run and be accessible to provide value, there is always a risk that a system's information or its control can be compromised.

Cyber hygiene does not address application-specific vulnerabilities, which include how threats such as Denial of Service, SQL injection, and so on, are handled by the application. Instead, Cyber hygiene provides a foundation for application security by addressing user, directory, and file security exposures in a general way; not targeted to any specific application. Cyber hygiene is run after product installation to correct these general vulnerabilities for system and application users, directories, and files. Any application used with the Linux operating system must be separately assessed for application-specific vulnerabilities.

The catalog of known vulnerabilities and exposures used in cyber hygiene is based on unclassified, non-confidential checklists from the United States Defense Information Services Agency (DISA). The items on these lists are assessed for applicability to cyber hygiene. Scanning scripts search for and log instances of an exposure and then, where applicable, the log files are used as input for remediation scripts addressing the problem. A small subset of security findings require different handling.

Documentation listing known vulnerabilities in IBM Intelligent Operations Center components, and the actions taken by cyber hygiene to mitigate them, is provided by IBM Intelligent Operations Center.

Related tasks:

“Checklist - installing using IBM Installation Manager” on page 14

Use this checklist to track the installation steps when installing IBM Intelligent Operations Center using IBM Installation Manager.

“Checklist - installing step-by-step” on page 15

Use this checklist to track the installation steps when installing IBM Intelligent Operations Center using scripts and commands.

“Installing IBM Intelligent Operations Center using Installation Manager” on page 25

IBM Intelligent Operations Center can be installed using the provided graphical installer.

“Installing and running cyber hygiene step-by-step” on page 58

Cyber hygiene is installed and run separately from IBM Intelligent Operations Center and must be installed and run after all other IBM Intelligent Operations Center components are installed, configured, and are operational. Cyber hygiene changes the default operating system configuration to a more secure set of options that help to assure a more secure foundation for the IBM Intelligent Operations Center system.

Cyber security

Securing the IT environment has long been a concern for national governments and is becoming increasingly important for critical infrastructure systems. Products and solutions providing critical infrastructure, such as IBM Intelligent Operations Center, should, where possible, have known vulnerabilities removed before those products and solutions are made available.

Cyber security is risk mitigation, not risk prevention. Since IT systems must be running and accessible to provide value, there is always some risk that a system’s information or control could be compromised. Cyber security consists of both static and dynamic elements. Cyber hygiene in IBM Intelligent Operations Center addresses the static elements of cyber security. Other tools and processes are needed to address the dynamic elements of cyber security. These tools and processes can include physical and personnel security procedures or network intrusion tooling.

The cyber hygiene capabilities provide by IBM Intelligent Operations Center are designed to address areas such as weak security configurations, software errors, system administration errors, and system security process errors. To provide this support, cyber hygiene provides installation and configuration features that configure the operating system and administration features that set secure settings and install key security-related fix packs. For example, systems are configured so no user IDs exist without a password and insecure Linux services, such as ftp, snmp, rlogin are disabled. However, systems cannot be automatically configured to meet specific enterprise security practices.

Cyber hygiene checklists

Cyber hygiene uses checklists based on unrestricted Defense Information Systems Agency (DISA) checklists and periodic vulnerability alerts.

Checklist item analysis

Each vulnerability identified in the unrestricted Defense Information System Agency (DISA) checklist defines data related to the vulnerability.

The information provided for each vulnerability include the following:

- A unique identifier. The identifier is made up of a Security Implementation Technical Guide (STIG) ID and a Vulnerability Management System (VMS) key.
- A short name summarizing the vulnerability.
- The severity of the vulnerability. Severity levels documented are:

I High severity

II Medium severity

III Low severity

- The affected product or products.
- The affected product version or versions.
- A description of the vulnerability including any use cases, context, or interactions with other software.
- Any recommended actions. If remediation is not available through a patch or an upgrade, a recommended mitigation might be included.
- Any alert that the alert supersedes.

For each vulnerability it is important to understand whether or not it affects IBM Intelligent Operations Center. For example:

- Is the product release and fix level included with IBM Intelligent Operations Center affected? An earlier product release or fix might not be affected since the issue could have been introduced in a later release or fix.
- Is the product included with IBM Intelligent Operations Center being used in a way that exposes the vulnerability? For example, a problem might only exist when the product is using services from another product. If those services are unused in the IBM Intelligent Operations Center configuration, then remediation might not be required.
- Does the product vulnerability affect the operating system being used? Some vulnerabilities may only exist when running specific operating systems.

For each item on a checklist, these factors were analyzed to determine the action required for IBM Intelligent Operations Center. This analysis and remediation results in one of four assessments:

Not Applicable (NA)

The affected product or configuration is not part of the IBM Intelligent Operations Center environment.

Not a Finding (NF)

The installed version and fix level of the product is not affected, or the product is not used in a way that exposes the vulnerability. This assessment is also used if the configuration does not expose the vulnerability.

Open The vulnerability applies to the installed product version and fix level, however, no remediation is available for the product. This assessment is also used if the system is configured in a way that exposes the vulnerability. For example, allowing world-write permissions on a directory because a product requires it.. This assessment is also used when applying a remediation might depend on organization policies such as password policies on length or character mix.

Fixed A remediation of an open vulnerability was applied and verified.

Table 27 shows an example analysis. The second example shows the handling of a product not installed on any IBM Intelligent Operations Center server.

Table 27. Example vulnerability assessments

| ID | Name | Severity | Application server | Event server | Data server | Management server | Explanation |
|-------------|--|----------|--------------------|--------------|-------------|-------------------|--|
| 2011-B-0082 | Multiple Vulnerabilities in IBM Websphere Application Server | I | NF | Open | NA | NF | Affects version prior to 6.1.0.39 and 7.0.0.19 |
| 2011-B-0085 | Multiple Denial of Service Vulnerabilities in Wireshark | I | NA | NA | NA | NA | Wireshark not installed |

Checklist selection

The checklists used for each server are based on the software installed on that server. Specific checklists address vulnerabilities for product types, for example, databases. Others address issues with specific products within a category, for example, DB2®.

Not all product types have specific checklists. Generic vulnerabilities are documented in the Application Security checklist or in an operating system-related list.

The following types of checklists are used by cyber hygiene:

Application security

Lists system level vulnerabilities. Some relate to the software development and testing practices and others address application-specific vulnerabilities such as not using encrypted passwords during user authentication.

Unix/Linux

Lists vulnerabilities related to configuration, password management, file system partitioning, and so on.

Web Server

Lists vulnerabilities related to HTTP servers.

Database

Lists vulnerabilities related to database servers.

Directory Servers

Lists vulnerabilities related to LDAP servers.

Enterprise System Management

Lists vulnerabilities related to enterprise system management tooling and system management processes.

Network security is not addressed by the checklists since network security configuration must be determined by a customer's policies and network architecture. Network security configuration must be handled according to the needs of each installation.

Cyber hygiene default configuration

The cyber hygiene feature sets Linux default configurations and policies to more secure options than are set in the default operating system installation. These default settings can easily be modified by system administrators to conform with the security policies for the installation.

An enterprise's IT operations administrative group is responsible for the security of their systems. This includes managing network access and internal security policies and processes.

Where the cyber hygiene default settings are inconsistent with enterprise policy, enterprise policies must take precedence. Remember that local security policy settings have not been tested for their impact on system functionality. The same care taken when applying security policy to products not deployed with cyber hygiene should be taken when applying security policy to IBM Intelligent Operations Center.

While IBM Intelligent Operations Center cannot be automatically be configured for individual enterprise security policies, IBM Intelligent Operations Center can be configured to remove known vulnerabilities. Cyber hygiene configures IBM Intelligent Operations Center with a set of default, best practice policies creating a foundation for system administrators to use when applying specific organizational policies and practices

Default password management policies

Cyber hygiene configures the default Linux operating system password management policies.

The default password management policies set by cyber hygiene are shown in Table 28.

Table 28. Default cyber hygiene password management policies

| Policy | Value or setting |
|-------------------------|--|
| Minimum password length | 8 characters |
| Accepted characters | uppercase letters, lowercase letters, numbers, special characters (: ; ! ` ~ @ # \$ % ^ & * () - _ = + [{] } \ ' " , < . > / ? and the space character) |

Table 28. Default cyber hygiene password management policies (continued)

| Policy | Value or setting |
|--|-----------------------------|
| Content rules | none |
| Number of failed log on attempts before locking out user | 3 |
| Minimum time between password changes | 1 day |
| Maximum time between password changes | 60 days |
| Are passwords required on accounts? | yes |
| When can a password be reused? | after 5 different passwords |
| Log in required after inactivity | 15 minutes of inactivity |
| Delay between log on failures | 4 seconds |

The `/etc/pam.d/system-auth` and `/etc/login.defs` files are modified when setting the cyber hygiene default policies.

These settings are intended to be the minimum necessary for reasonable security practices. You should modify these settings to match your organization's security policies. Some areas where you might want to change the default settings are as follows:

- While the default configuration sets the minimum password length to 8 characters, best practices for secure systems generally considers secure passwords to be 14 or more characters in length.
- The maximum time between password changes should be set to a value appropriate for your organization. This is defined in the **inactive** parameter in the `/etc/shadow` file. At the defined point in time the user is forced to change the password at log on. If the user fails to change the password, the password must be reset by a privileged user. Whether the value specified in the `/etc/shadow` file is used depends on the default action specified in the `/etc/default/useradd` file. If the `/etc/default/useradd` file specifies `-1`, the password does not expire. If `/etc/default/useradd` specifies `0`, the account is locked. If any other value in the `/etc/default/useradd` file is defined, the **inactive** parameter value in the `/etc/shadow` is used for the password expiration.
- Rules concerning the complexity and content of passwords should be addressed and implemented according to the enterprise security policy.

See the Linux documentation for more information on managing password policies.

Disabled Linux services

Cyber hygiene disables or uninstalls vulnerable Linux services. These services can allow system access and should only be started or installed if there is a need for them.

The following Linux services (daemons) are not started by default. They can be started if needed.

- `inetd/xinetd`
- `portmap`
- `avahi-daemon`
- `bluetooth`
- `cups`
- `hidd`
- `isdn`
- `rhnsd`
- `canna`
- `pcmcia`
- `yplib`

- autofs
- smartd
- netfs
- snmpd
- nfs
- samba

These services can be started using the **service** *service_name* **start** command.

Note: These services, if not properly configured, can be compromised and allow unauthorized access to the system. This is why, for system security, they are not started by default.

The following Linux services are removed. They can be reinstalled if needed using the **rpm** or **yum** commands. For example, the **yum install httpd** command will install the HTTP daemon package.

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod_python
- mod_perl
- mod_ssl
- webalizer
- httpd-manual

Note: These services are removed from Linux because they have a high potential for causing security exposures in server environments.

Removed user IDs

A standard Linux installation contains a number of user IDs that are not desirable in a secure production environment. Cyber hygiene removes these user IDs from the Linux user registry and `/etc/passwd` file. The associated home directories are also removed.

The following user IDs are deleted and can be recreated if needed.

- games
- news
- ftp
- halt
- shutdown
- reboot
- who
- gopher
- lp
- rpcuser
- uucp

If these user IDs are required, standard Linux administration procedures can be used to create them.

Audit rules

Standard auditing in Linux is minimal since audit files can quickly grow. However, when security is an issue, additional auditing is critical to be able to determine what happened in an incident. Cyber hygiene scripts add a set of additional audit rules for all Linux run levels. Events matching these rules will be logged into the standard system log files.

The following Linux audit rules are added and can be modified if needed.

- Failed attempts to access programs and files
- Deletion of programs and files
- Administrative, security, and privileged actions
- Access control permission changes

Having good audit logs is a good security practice. If for some reason the auditing defined by cyber hygiene needs to be changed, the `/etc/audit/auditd.conf` and `/etc/audit/audit.rules` files need to be modified. Cyber hygiene turns on auditing for all five runtime levels of Red Hat Enterprise Linux.

File and directory permissions

Cyber hygiene changes existing file and directory permissions to meet security best practices.

The file and directory permission changes made by cyber hygiene are as follows:

Restriction of system scripts

Sensitive security system scripts cannot be accessed by users without the appropriate privileges.

Removal of world-write permission

Users cannot write to directories that are not public. Applications and users needing to modify files and directories must be the owner, or a member of the group, for the file or directory.

Removal of world-read and execute permission

The world-readable and world-executable permissions are removed for many files and directories. In particular, these permissions are removed from user home directories. Applications and users needing to read or run files must be the owner, or member of the group, for the file or directory.

Other changes

Cyber hygiene makes other changes to address security exposures.

Batch programs - at command

To stop non-privileged users from using the `at` command to run batch programs at a particular time, cyber hygiene deletes the `at.deny` file and creates an empty `at.allow` file.

The `at.allow` file defines the users allowed to run the `at` command. An `at.allow` file containing no user IDs implies that no users, other than privileged system IDs, can run the `at` command. If the `at.deny` file, which defines users explicitly not allowed to use the `at` command, exists, but the `at.allow` file does not exist, then all users, except those in the `at.deny` file, are allowed to run the `at` command. If neither file exists, only the superuser can run the `at` command.

By default Red Hat Enterprise Linux is configured to allow users to execute the `at` command.

Batch programs - cron command

Users without administrative privileges are not allowed to run the **cron** command to schedule batch programs.

Ctrl-Alt-Del

The Ctrl-Alt-Del key combination is disabled so it cannot be used to shut down the system.

Remediation tools

IBM Intelligent Operations Center cyber hygiene functionality provides remediation tools to correct vulnerabilities in the installed IBM Intelligent Operations Center system.

Remediation tools are run when cyber hygiene is run after IBM Intelligent Operations Center installation is complete. These tools can also be run when the system is in production to find and correct vulnerabilities that might be created when other products are installed on the servers or as a result of system use.

Vulnerability scanner

The scanner consists of scripts that review the IBM Intelligent Operations Center system and identify vulnerabilities. For example, the scanner identifies directories with write privileges for any user.

The scanner creates a findings file used by the remediation scripts. The findings file lists identified vulnerabilities within the IBM Intelligent Operations Center system.

The scanner scripts do not make changes to the IBM Intelligent Operations Center system. The scanner only identifies vulnerabilities. It can be used after remediation to validate the changes made by the remediation scripts.

Vulnerability remediation scripts

Cyber hygiene has three types of remediation scripts:

- Scripts that make configuration changes which do not require scanning, which can be easily reversed, or have no noticeable runtime impact on the system. For example, changing the default file access permission of the man pages to 644.
- A script to disable remote logon with the root account.
- A script that processes the findings file created by the scanner and resolves identified vulnerabilities. Care should be taken in using this script after additional products are installed. Some products require less strict settings and can malfunction after these scripts are run. Review the findings files created by the scanner scripts for potential risks before running any remediation scripts.

Remediation logs

Scanning and remediation scripts log their actions in four log files on each IBM Intelligent Operations Center server. These logs are located in the `/var/BA15/CH/results` directory. Subdirectories contain working copies of the scan and remediation results.

The scanner is run twice: once to remediate vulnerabilities and a second time to log remediations not done. The log from the second run can be used by the administrator to determine if manual remediation steps are required.

Cyber hygiene documentation

Documentation is available to help the customer evaluate the changes applied to the installed IBM Intelligent Operations Center system. This documentation assists with the certification and accreditation of systems for production use.

Documentation includes an overview of the overall cyber hygiene strategy, the rationale for why some defaults were implemented, and a spreadsheet documenting the status of each DISA flagged vulnerability. The spreadsheet can be used during product security assessments.

Related information:



Cyber hygiene implementation in IBM Intelligent Operations Center 1.5

Chapter 4. Integrating the solution

Products and services can be integrated with the IBM Intelligent Operations Center incorporating data related to events.

Event data communicated to the IBM Intelligent Operations Center can be in the Common Alerting Protocol or other protocols.

Events can be related to key performance indicators (KPI) monitored by the IBM Intelligent Operations Center. Events in the IBM Intelligent Operations Center can be related also to standard operating procedures and available resources. The solution provides a report administration service so that you can produce up-to-date reports and summaries of your event data.

Examples of systems that can be integrated

Products and services can be integrated with the IBM Intelligent Operations Center.

Examples of systems and services include:

- Systems reporting on public safety issues.
- Systems reporting on traffic events.
- Systems reporting on water quality and usage.
- Systems providing data on outages and status of related work orders.

These systems must be able to communicate with the IBM Intelligent Operations Center and send events and measurements in the supported protocol to the IBM Intelligent Operations Center inbound event queue.

Related concepts:

“Using the inbound event queue defined for the IBM Intelligent Operations Center” on page 95
CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

“Integrating with the Common Alerting Protocol” on page 89

The Common Alerting Protocol (CAP) is used to exchange event information between the IBM Intelligent Operations Center and external systems.

Integration points and protocols

Other systems can be integrated with the solution through the IBM Intelligent Operations Center services and policies. Data can be received in the Common Alerting Protocol (CAP) format; other protocols are also supported.

Events and KPIs

The IBM Intelligent Operations Center processes events and key performance indicators (KPIs) to determine how information is displayed.

Other products and services can be integrated with the IBM Intelligent Operations Center through the message bus service. KPIs are monitored by the business monitoring service.

Events are received by the IBM Intelligent Operations Center. These events can be displayed on a Details portlet and can affect what is displayed on map portlets.

KPI definition determines how KPIs are displayed on Status and Key Performance Indicator Drill Down portlets. KPI definition can also determine how information about events is displayed. For example, if a KPI threshold is exceeded, the event might be flagged with a higher urgency or severity. Events without corresponding KPI definitions are displayed according to the information received about the event.

For more information about how KPIs are created and integrated, see the link at the end of this topic.

Related concepts:

“Creating and integrating KPIs” on page 105

Key performance indicator (KPI) models can be created and modified using a business monitoring development toolkit and a KPI management portlet.

Policy for KPI updates

The IBM Intelligent Operations Center policy determines if an incoming event is a KPI event update, then sends it for processing to generate a KPI update or an alert depending on parameters. A KPI event is determined by `<code>KPI</code>` in the alert block of the Common Alerting Protocol XML.

If the event is confirmed as a KPI update, the policy checks the KPI parameters and generates a KPI event XML to send to the IBM WebSphere Business Monitor for processing.

The following table shows a sample KPI event update.

Table 29. Sample KPI event properties

| Property | Value |
|-----------------------|---|
| Sender | security@rtp.city.gov |
| Event type | Crime Response Time |
| Event status | Actual- actionable by all target recipients |
| Event scope | Public - For general dissemination to unrestricted audiences |
| Category | Security |
| Severity | Severe |
| Certainty | Likely |
| Urgency | Immediate |
| Message type | Alert- initial information requiring attention by targeted recipients |
| Description | Burglary |
| Sent date / time | 2012-02-17T17:06:00+01:00 |
| Onset date / time | 2012-02-16T15:47:00+01:00 |
| Responded date / time | 2012-02-17T17:06:00+01:00 |

The following table shows the sample KPI parameters associated with the KPI event update in Table 29.

Table 30. Sample KPI event parameters

| Parameter | Value |
|---------------|---------------------------|
| Report Number | 1111 |
| Precinct | Precinct One |
| Responded | 2011-02-15T15:05:07-05:00 |

Related concepts:

“Status” on page 274

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

“Notifications” on page 271

Use the Notifications portlet to view your alert messages and their details.

Integrating with the Common Alerting Protocol

The Common Alerting Protocol (CAP) is used to exchange event information between the IBM Intelligent Operations Center and external systems.

The CAP is a generic format for exchanging emergency alerts and public warnings over various networks. It provides an open, non-proprietary digital message format for all types of alerts and notifications. The CAP is compatible with emerging techniques, such as web services, while offering enhanced capabilities. These capabilities include:

- Flexible geographic targeting using latitude and longitude shapes and other geospatial representations in three dimensions
- Multilingual and multi-audience messaging
- Phased and delayed effective times and expirations
- Enhanced message update and cancellation features
- Template support for framing complete and effective warning messages
- Digital encryption and signature compatibility
- Digital images and audio facilities

Events are self-contained data messages that can be sent or consumed by all components. Events can be published to topic queues and read by all potentially interested subscribing IT systems. The CAP helps standardize event content so multiple domains can send and receive events in a common format using common conventions. The standard defines the mandatory and optional fields in the event record and the acceptable values for those fields. Event processing management can mediate between legacy formats and the standardized format. The CAP can be extended to handle day-to-day operations in addition to emergency situations.

Minimally, events must contain:

- A unique event identifier that contains:
 - The sender (system or human)
 - Organization sending the event
 - Serial number within sending system
 - Timestamp of event creation
- Information that allows recipients to define and prioritize responses:
 - Urgency – how rapidly recipients should respond to the alert
 - The level of threat to life and property
 - Certainty – a probability ranging from 100%, the event has been observed, to 0%, the event is now not expected to occur
 - Predicted time for events that might happen in the future
 - Duration of events that have been previously reported and whose continuation is being reported
 - Anticipated duration of events that represent a situation that cannot be corrected promptly
 - Recommended or mandated actions and directives
- Information to allow the event to be correlated:
 - City semantic model references (if one exists)

- Geospatial coordinates
- Reference to prerequisite event, or an event that was the precipitating cause
- Unique asset identifiers for any involved
- Human readable textual descriptions:
 - Location description
 - Activity description

Using the CAP helps minimize per-event data exchange. Because events are formatted in XML, the data format can be written and read by a variety of systems thereby preventing the exchange of meaningless data or data creating dangerous confusion.

The IBM Intelligent Operations Center provides persistent storage of CAP alerts and a standard interface for presenting them.

While the entire CAP structure is accepted by the IBM Intelligent Operations Center, only some data is used by the IBM Intelligent Operations Center when calculating key performance indicators (KPI).

The IBM Intelligent Operations Center uses the WebSphere Message Broker to integrate events using the CAP.

The IBM Intelligent Operations Center supports OASIS Common Alerting Protocol Version 1.2.

Related concepts:

“Using CAP for KPI events” on page 92

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

“Using CAP for non-KPI events” on page 95

You can also use CAP data to provide data on events not associated with KPI calculations.

Related information:

 [OASIS Common Alerting Protocol Version 1.2](#)

CAP structure

Each CAP alert message consists of an <alert> segment that can contain one or more <info> segments. Each <info> segment can include one or more <area> segments. In most cases, CAP messages with a <msgType> with a value of *alert* includes at least one <info> element.

The following are the main message elements.

- <alert>

The <alert> segment provides basic information about the current message: its purpose, its source, and its status. It also has a unique identifier for the message and links to any other related messages. An <alert> segment can be used alone for message acknowledgments, cancellations, or other system functions; however, most alert segments include at least one <info> segment.
- <info>

The <info> segment describes an anticipated or actual event in terms of urgency (the time available to prepare), severity (the intensity of the impact) and certainty (confidence in the observation or prediction). It also provides both categorical and textual descriptions of the subject event. The <info> segment might also provide instructions for appropriate response by message recipients and other details, for example hazard duration, technical parameters, contact information, and links to additional information sources. Multiple <info> segments can be used to describe differing parameters, such as different probability or intensity bands, or to provide the information in multiple languages.
- <resource>

The <resource> segment provides an optional reference to additional information related to the <info> segment. It might reference a digital asset such as an image or audio file.

- <area>

The <area> segment describes a geographic area to which the <info> segment applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes, polygons and circles, and an altitude or altitude range expressed in standard latitude, longitude, and altitude terms in accordance with a specified geospatial datum.

Related concepts:

“Using CAP for KPI events” on page 92

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

“Using CAP for non-KPI events” on page 95

You can also use CAP data to provide data on events not associated with KPI calculations.

Event types

Several CAP event types are supported by the IBM Intelligent Operations Center.

Actual/predicted event

Actual/predicted event messages are unsolicited messages sent by various domains about abnormal conditions or exceptions. These messages also cover key performance indicator (KPI) violations where an event is created.

Acknowledgement

An acknowledgement is a CAP message with the following field values in the <alert> element:

- The <msgType> value is set to **ACK** which means the sender acknowledged the receipt and acceptance of the messages identified in <references>.
- The <references> field contains the extended message identifiers (in the format sender, identifier, sent) of an earlier CAP message or messages referenced by the acknowledgement.
-

Note: The <info> element is optional for an acknowledgement.

Response

A response is a CAP message with the following field values in the <alert> element:

- The <msgType> value is **Alert**.
- The <note> value is **Response**.
- The <references> element must contain the identifiers of the CAP message to which this is a response

For example, when a city operator sends a **City Brownout Advisory** to various domains, those domains send back a response to the advisory after performing an impact analysis on their individual functions.

Incident

Incidents are used to collate multiple messages referring to different aspects of the same incident. Incident CAP messages act as a container of all the events that are related to an specific incident. These events can be in different domains.

An advisory is promoted to an incident when domains send back responses to the advisory indicating multi-domain impacts requiring a coordinated action. The <incident> element in all related events is populated with the <identifier> value of the incident event. Related events are events where the <references> value is the same as the <identifier> value of the incident event.

An incident is a CAP message with the following field values in the <alert> element:

- The <msgType> value is **Alert**.
- The <note> value is **Incident**.
- The <references> element must contain the identifiers of the CAP message that is the parent (the root cause) of this event
- The <incidents> element must contain its own identifier

Update

An update is a CAP message with the following field values in the <alert> element:

- The <msgType> element is set to **update** which means that this update supersedes the earlier messages identified in the <references> element.
- The <references> element contains the extended message identifiers (in the format sender,identifier,sent) of an earlier CAP message or messages referenced by the update.

Cancel

A cancel is a CAP message with the following field values in the <alert> element:

- The <msgType> element is set to **Cancel** which means that this message cancels the earlier messages identified in the <references> element.
- The <references> element contains the extended message identifiers (in the format sender,identifier,sent) of an earlier CAP message or messages referenced by this cancelation.
- The <note> element contains an explanation of why or how this alert is cleared.

Related information:

 [OASIS Common Alerting Protocol Version 1.2](#)

Using CAP for KPI events

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

Table 31 lists the data elements used in KPI calculations:

Table 31. CAP elements used in IBM Intelligent Operations Center KPI calculations

| Required or Optional | Data Element (normative) | Description |
|----------------------|--------------------------|---|
| Required | Message_ID (identifier) | Unique message identifier |
| Required | Sender_ID (sender) | Unique sender identifier |
| Required | SentDateTime (sent) | Date and time the message was sent. For example: 2011-02-07T 16:49:00-05:00 contains the date and time a message sent. The last six characters indicate the CAP event time zone, in relation to Greenwich Mean Time (GMT). In this case, the event occurred at 16:49:00, at GMT minus 5 hours, which is Eastern Standard Time (EST). This code means that when the event is displayed, it is converted from EST to the user's time zone. If you want to code your CAP events in GMT instead, change the suffix to -00:00 as in this example: 2011-02-07T 16:49:00-00:00. |

Table 31. CAP elements used in IBM Intelligent Operations Center KPI calculations (continued)

| Required or Optional | Data Element (normative) | Description |
|----------------------|--------------------------|---|
| Required | MessageStatus (status) | Status of the message, can be one of the following options: <ul style="list-style-type: none"> • Actual • Exercise • System • Test • Draft |
| Required | MessageType (msgType) | Type of the message, can be one of the following options: <ul style="list-style-type: none"> • Alert • Update • Cancel • Ack • Error |
| Optional | Source (source) | Source of the message |
| Required | Scope (scope) | Contains the value Public |
| Required | Code (code) | Contains the value KPI to hide this event from the Events portlet list. |
| Required | EventCategory (category) | One of the following: <ul style="list-style-type: none"> • Geo • Met • Safety • Security • Rescue • Fire • Health • Env • Transport • Infra • CBRNE • Other |
| Required | EventType (event) | Description of the event or KPI. For example: Police_Department_Budget |
| Required | Urgency (urgency) | One of the following: <ul style="list-style-type: none"> • Immediate • Expected • Future • Past • Unknown |

Table 31. CAP elements used in IBM Intelligent Operations Center KPI calculations (continued)

| Required or Optional | Data Element (normative) | Description |
|----------------------|--------------------------------|---|
| Required | Severity (severity) | Severity is indicated by one of the following options: <ul style="list-style-type: none"> • Extreme • Severe • Moderate • Minor • Unknown |
| Required | Certainty (certainty) | Certainty is indicated by one of the following options: <ul style="list-style-type: none"> • Observed • Likely • Possible • Unlikely • Unknown |
| Optional | EventCode (eventCode) | Name-value pairs for event typing. |
| Optional | OnsetDateType (onset) | Date and time the event begins For example: 2011-02-08T16:49:00-05:00 |
| Optional | SenderName (senderName) | Name of the entity which initiated the alert. For example: Police Department |
| Optional | EventDescription (description) | Detailed description of the event or KPI |
| Optional | Parameter (parameter) | Additional data associated with the event or KPI. |
| Optional | AreaGeocode (geocode) | A field that can be used to provide information when the event or KPI is location-dependent |

For more information, see the related link at the end of this topic to the OASIS Common Alerting Protocol specification.

The following code is an example of an event that reports a car accident.

```
<?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>1112</cap:identifier>
  <cap:sender>Transportation</cap:sender>
  <cap:sent>2011-02-17T15:00:00-05:00</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>Transport</cap:category>
    <cap:event>Traffic_Accident</cap:event>
    <cap:urgency>Unknown</cap:urgency>
    <cap:severity>Extreme</cap:severity>
    <cap:certainty>Unknown</cap:certainty>
    <cap:eventCode>
      <cap:valueName>OwningOrg</cap:valueName>
      <cap:value>Police</cap:value>
    </cap:eventCode>
    <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
    <cap:senderName>Transportation</cap:senderName>
    <cap:description>Single car crash</cap:description>
  </cap:info>
</cap:alert>
```

```

<cap:parameter>
  <cap:valueName>accident number</cap:valueName>
  <cap:value>1112</cap:value>
</cap:parameter>
</cap:info>
</cap:alert>

```

Related concepts:

“Localizing the user interface” on page 135

Browser settings determine language, date and time settings for the IBM Intelligent Operations Center user interface. An administrator can customize the date and time formats.

“Known problems and solutions” on page 310

This section contains a list of commonly occurring problems and a solution for each item.

Related information:

 [OASIS Common Alerting Protocol Version 1.2](#)

Using CAP for non-KPI events

You can also use CAP data to provide data on events not associated with KPI calculations.

CAP data received by the IBM Intelligent Operations Center that is not associated with defined KPIs is added to the Events and Map portlets in the IBM Intelligent Operations Center.

The following code is for an example non-KPI event. Note that for non-KPI events, you must set the value of the code tag to Event.

```

<p>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>
  <sender>TestGenerator</sender>
  <sent>2012-03-26T15:47:24-00:00</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>Immediate</urgency>
    <severity>Moderate</severity>
    <certainty>Observed</certainty>
    <headline>Major water line leak at NW 20th St.</headline>
    <description>Leak is located at the intersection of NW 20th Street and NW 9th Avenue. Street flooding starting to occur. Immediate action required.</description>
    <area>
      <circle>25.79518,-80.21110 0</circle>
    </area>
  </info>
</alert>
</p>

```

Using the inbound event queue defined for the IBM Intelligent Operations Center

CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

Publishing clients can be configured to point directly to the WebSphere Message Broker CAP event input queue, or they can use the WebSphere Application Server JMS resources defined on the portal server. These JMS resources point to the WebSphere Message Broker queue that receives CAP events. The following JMS resources are created when the IBM Intelligent Operations Center is installed:

- Queue Connection Factory

- Name: ioc.mb.con.factory
- JNDI Name: jms/ioc.mb.con.factory
- Queue
 - Name: ioc.cap.in.q
 - JNDI Name: jms/ioc.cap.in.q

Related concepts:

“KPI event communication between IBM WebSphere Business Monitor and IBM Intelligent Operations Center” on page 112

IBM WebSphere Business Monitor can send outbound events from a monitoring or key performance indicator (KPI) context to IBM Intelligent Operations Center.

Creating events using the Publisher service

You can submit events to IBM Intelligent Operations Center through web services to the Publisher service.

You can create client applications that can be integrated into a deployed instance of IBM Intelligent Operations Center. You can use a client application to pass CAP alerts from a third-party client application into IBM Intelligent Operations Center by calling the methods exposed by the Publisher service utility class and the IBM Intelligent Operations Center Publisher servlet.

Developing with the common utility classes

If you want to create a client application that calls the Publisher service, before you begin you must set up the common utility classes. After you finish developing your client application, export it as a WAR file that you then import into WebSphere Application Server.

About this task

Use the following procedure if you want to develop a client application with the common utility classes:

- Before developing your client application, add the `iss_common` and `icu4j-4_4_2` JAR files to the project build path. The JAR files are required during compile time.
- After developing your client application, export it as a WAR file.
- Import the WAR file into WebSphere Application Server, and configure it to reference the shared libraries.

Procedure

1. Locate the `iss_common.jar` file and the `icu4j-4_8_1_1.jar` file in the IBM Intelligent Operations Center installation directory, `/opt/IBM/iss/common/lib`.
2. Copy the `iss_common.jar` file and the `icu4j-4_8_1_1.jar` file to a location on your development machine.
3. To add the JAR files to the project build path, in the IBM Intelligent Operations Center API, do the following substeps for `iss_common.jar` and `icu4j-4_8_1_1.jar`:
 - a. Right-click the **Portlet Project**.
 - b. Click **Build Path** > **Configure Build Path**.
 - c. Click the **Libraries** tab, and click **Add External JARs...**
 - d. Browse to the directory that contains the JAR file.
 - e. Click the JAR file, and then click **Open**.
4. When you have finished developing your client application, export it as a WAR file.
5. In the WebSphere Application Server administrative console, use the import wizard to import the client application WAR file.
6. To configure the WAR file to reference the shared library references, do the following substeps:

- a. In the WebSphere Application Server administrative console, select the check box beside your imported WAR file, and then click **Update**.
- b. Click **Shared library references**.
- c. On the Shared library references window, select the **Application** check box.
- d. Click **Reference shared libraries**.
- e. Move **ISSCommonJars** and **IOCCCommonJars** from the Available list to the Selected list, and then click **OK**.
- f. To save your changes, click **OK**.

Using the Publisher service

The Publisher service event injector tool is provided as a Java utility. You can create a client application that passes CAP XML into the IBM Intelligent Operations Center by calling the methods exposed by the Publisher service. You can also pass in notifications.

The Publisher service is a utility class in the project `iss_common_utils`, which is built into the `iss_common.jar` file. The Publisher service exposes the static methods `publishEvent` and `publishNotification`. Before you create client applications for the Publisher service, you must set up the common utility classes. For more information, see the link at the end of the topic.

To ensure that the code used to call the Publisher service has access to the correct JMS queue configurations, you must deploy it on the application server.

The following sample code shows how to call the Publisher service:

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);

if (status == Publisher.STATUS_SUCCESS) {
    logger.traceFine(this, methodName, "Event submit request was performed successfully");
}
else if (status == Publisher.STATUS_EXCEPTION_NAMING) {
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Requires defining JMS Resources.");
}
else if (status == Publisher.STATUS_EXCEPTION_JMS) {
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Failed to connect to JMS resources.");
}
else { //Other error code
    logger.traceFine(this, methodName, "Error sending CAP Event Message. Returned status = " + status);
}
```

If you use the Sample Publisher portlet, it is not necessary to create the code to call the Publisher service, or to write any CAP messages.

Related concepts:

“Sample Publisher” on page 99

Use the Sample Publisher portlet to publish Common Alerting Protocol (CAP) events into the IBM Intelligent Operations Center.

Related tasks:

“Developing with the common utility classes” on page 96

If you want to create a client application that calls the Publisher service, before you begin you must set up the common utility classes. After you finish developing your client application, export it as a WAR file that you then import into WebSphere Application Server.

Using the Publisher servlet

The Publisher servlet accepts parameters in POST requests to publish CAP XML, create new events, or create modified events from existing events or incidents.

Sending POST requests to the Publisher servlet

The Publisher servlet calls the Publisher service to put the CAP XML on the queues that feed into the IBM Intelligent Operations Center. The Publisher servlet is located at `/ibm/iss/common/rest/publisher`. The following table shows how to send POST requests to the Publisher servlet.

Table 32. Publisher servlet POST requests

| Type of event to be published | POST request code |
|-------------------------------|---|
| Publish a new CAP event | <code>action=publishEvent&source=xml&xml=CAP_event_XML</code> |
| Modify an existing event | <code>action=publishEvent&source=existing&id=event_id</code> |
| Publish a blank new event | <code>action=publishEvent&source=new</code> |

Optional parameters

You can apply optional parameters to each of the publish options by appending the following code to the POST request: `¶meter_name=new_value`

The following optional parameters are available:

- areaDesc
- category
- certainty
- code
- contact
- description
- event
- headline
- latitude
- longitude
- msgType
- randomize
- randomizeid
- randomizeArea
- randomizeTime
- sender
- senderName
- severity
- status
- urgency

For example, to publish a blank new event, and then set the headline to Traffic, the POST request code is: `servletURL&action=publishEvent&source=new&headline=Traffic Accident`

Creating and publishing test events

The IBM Intelligent Operations Center provides the Sample Publisher portlet and the Event Scripting portlet for creating and publishing test events.

Related concepts:

“Creating events using the Publisher service” on page 96

You can submit events to IBM Intelligent Operations Center through web services to the Publisher service.

Sample Publisher

Use the Sample Publisher portlet to publish Common Alerting Protocol (CAP) events into the IBM Intelligent Operations Center.

The Sample Publisher portlet is an automated test tool intended for an administrator managing or verifying the solution. An administrator can use the Sample Publisher portlet as a client application to test the publication of CAP messages in the IBM Intelligent Operations Center. The Sample Publisher portlet can eliminate the requirement to manually create a test client application.

Creating events and notifications

To launch the Sample Publisher portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Sample Event Publisher**.

On the **Event CAP** tab of the Sample Publisher portlet, you can complete a form to design events with XML. Submit the form to activate a flow of sample CAP events into the system.

The Sample Publisher portlet also contains an **Event Form** tab for creating new events when it is not necessary to edit the XML. Complete the form in the **Event Form** tab to submit the CAP event details. If you want to create new events with properties based on the properties of an existing event, enter the CAP Alert ID for the existing event in the **ID** field.

The Sample Publisher portlet contains a **Notification** tab for testing the notifications subsystem of the IBM Intelligent Operations Center. On the **Notification** tab, you can complete a form to submit an alert notification for specified groups. The values you enter in the **Sent To Groups** field must match existing user groups, for example, `CityWideOperator`, `CityWideExecutive`, because only matching alerts are displayed in the Notifications portlet list.

Random values

On the **Event CAP** and **Event Form** tabs, if you select the **Randomize Events** check box, the portlet automatically alters the properties of the events it publishes as follows:

- **ID**: the portlet generates a unique ID string for each event because event IDs must be unique in the IBM Intelligent Operations Center.
- **Timestamp**: The portlet increments the value of the timestamp for each event sent so that each event in the sequence arrives at a different time.
- **Location**: The portlet randomizes the latitude and longitude for each event, within a range, to comply with the format required for latitude, longitude, and radius; for example, `32.9525,-115.5527 5`. The radius setting is not changed.

Customizing the Sample Publisher portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related reference:

“Sample Publisher portlet settings” on page 155

Customize the Sample Publisher portlet by changing the settings in the fields of the **Shared Settings** window.

Creating sample events with XML

On the **Event CAP** tab, you can select a sample CAP event template that you can use to view, modify, and publish events.

Before you begin

Initially, choose an event category. The categories represent the primary areas into which events are divided.

Table 33. Event categories

| Category | Description |
|----------------|---|
| CBRNE | Chemical, biological, radiological, nuclear, or high-yield explosive threat or attack |
| Environmental | Pollution and other environmental event |
| Fire | Fire suppression and rescue |
| Geophysical | Geophysical event, including landslide |
| Health | Medical and public health event |
| Infrastructure | Utility, telecommunication, or other non-transport infrastructure event |
| Meteorological | Meteorological event, including flood |
| Rescue | Rescue and recovery |
| Safety | General emergency and public safety |
| Security | Law enforcement, military, homeland, and local/private security |
| Transportation | Public and private transportation |
| Other | Other events |

About this task

For more information about event properties, see the link at the end of the topic to the Details portlet topic.

Procedure

1. In the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Sample Event Publisher**.
2. Click the **Event CAP** tab.
3. From the **Category** list, select an event category.
4. For the **Event Message** field, choose one of the following options:
 - To insert the XML for the corresponding prewritten CAP message automatically into the **Event Message** field, from the **Sample Event** list, select an event. If you want, edit the XML to suit your requirements.
 - In the **Event Message** field, manually enter the XML for the CAP message from scratch.
5. In the **Event Instance Count** field, either enter the number of messages required, or use the arrows to select the number of messages required. You can submit a single CAP message or an automated sequence of messages.

6. Optional: Select the **Randomize Events** check box. If you select **Randomize Events**, a sequence of CAP messages is published with random IDs applied. The messages are published at incremental time intervals, and in random locations within a range.
7. Click **Submit Event**.

Results

The Sample Publisher populates the IBM Intelligent Operations Center with events and can trigger KPIs.

Related concepts:

“Details” on page 257

Use the Details portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

Creating new CAP events or updating existing events without XML

On the **Event Form** tab, you can complete a form to create new CAP events or update existing events, without using XML.

About this task

You can use the form to create either a new event or an event based on the values from an existing event. When you create an event based on an existing event, you use the CAP Alert ID to reference the existing event. Any values that you enter on the form override values inherited from the existing CAP event. For more information about event properties, see the link at the end of the topic to the Details portlet topic.

Procedure

1. In the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Sample Event Publisher**.
2. Click the **Event Form** tab.
3. To specify a source for the event, next to Source click one of the following options:
 - To create a new event with values based on the values you enter in the form, click **New**.
 - To create an event with values based on an existing event in the CAP events table and using the CAP Alert ID, click **Existing**.
4. In the **ID** field, enter an ID depending on whether you are creating a new event, or an event based on an existing CAP Alert ID:
 - If you are creating a new event, optionally enter a value for **ID**. If you do not enter a value, a unique identifier is generated for you.
 - If you are creating an event based on an existing CAP Alert ID value, enter the CAP Alert ID value for **ID**. Any values that you enter on the form override values inherited from the existing CAP event.
5. If you are creating a new event, in the **Event Type** field, enter one of the following event types:
 - Alert** A new event.
 - Update**
An update to a previously created event.
 - Cancellation**
A cancellation of a previously created event.
6. In the **Headline** field, enter a headline.
7. From the **Message Type** list, select a message type.
8. If you are creating a new event, from the **Event Code** list, select **Event** or **Incident**. An incident has higher importance than an event.
9. From the **Category** list, select a category.
10. From the **Urgency** list, select the urgency.

11. From the **Severity** list, select the severity.
12. From the **Certainty** list, select the certainty.
13. In the **Description** field, enter a description.
14. In the **Sender** field, enter a description of the sender of the event.
15. In the **Event Instance Count** field, select the number of messages required. You can submit a single CAP message or an automated sequence of messages.
16. Optional: Select the **Randomize Events** check box. If you select **Randomize Events**, a sequence of CAP messages is published with random IDs applied. The messages are published at incremental time intervals, and in random locations within a range.
17. Click **Submit Event**.

Related concepts:

"Details" on page 257

Use the Details portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

Testing notifications

Use the **Notification** tab to create test notifications for testing the notifications subsystem in the IBM Intelligent Operations Center.

About this task

On the **Notification** tab, complete the form to submit an alert for specified groups. For a particular user, an alert notification message is displayed in the Notifications portlet only if the user is a member of one of the Sent To Groups specified in the notification.

Procedure

1. In the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Sample Event Publisher**.
2. Click the **Notification** tab.
3. To create an alert, from the **Type** list, select **Alert**.
4. Optional: From the **Category** list, select a category.
5. Optional: In the **Headline** field, enter a headline.
6. Optional: In the **Description** field, enter a description.
7. Optional: In the **Sender** field, enter a description of the sender of the event.
8. Optional: In the **Sent to Groups** field, enter a semicolon-separated list of groups to send the alert to, for example, `;CityWideOperator;CityWideExecutive;`.

Note: In addition to inserting a semicolon between each group name, ensure that you insert a semicolon at the beginning of the list and at the end of the list.

When published, this alert notification is displayed in the Notifications portlet only for users who are members of the `CityWideOperator` and `CityWideExecutive` groups.

9. Optional: Do one of the following steps as required:
 - In the **Refers to Alerts** field, enter a semicolon-separated list of CAP event identifiers that the new alert refers to.
 - In the **Refers to KPIs** field, enter a semicolon-separated list of KPIs that the new alert refers to.
10. Click **Submit Notification**.

Related concepts:

“Notifications” on page 271

Use the Notifications portlet to view your alert messages and their details.

Event Scripting

Use the Event Scripting portlet to write a script to create a sequential list of events to be published at predefined time intervals.

To launch the Event Scripting portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Event Scripting**.

In the Event Scripting portlet, you can write a script that references events to be published by the event IDs that are recorded in the sample events table in the IBM Intelligent Operations Center database. In the script, you can specify a delay between the events to be published. When you run the script, the system publishes the events through the back end. However, the event flow is the same as for events that enter the system from external sources.

You can also clear the events from the IBM Intelligent Operations Center database. If you clear the events from the IBM Intelligent Operations Center database, all the events that are displayed in the Map portlet and the Details portlet are deleted.

Before you use the Event Scripting portlet, you can view the events in the sample events table in the IBM Intelligent Operations Center database.

In the Event Scripting portlet, follow the example to create a JSON script that defines a sequential list of events to be published at predefined time intervals. Before running the script, you must clean up and validate the script by clicking the **Clean Up and Validate** button.

You can publish an event with a particular ID only once. You must delete all the events from the IBM Intelligent Operations Center database before you can publish an event with the same ID again. However, if you select the **Randomize IDs** check box, the event scripting portlet publishes the same events again, and applies random IDs to the events.

Viewing sample events and KPI events in the sample events table

The Event Scripting portlet publishes sample events from the sample events table in the IBM Intelligent Operations Center database. Use the following procedure to view the events in the sample events table.

Procedure

1. Use a VNC client to log on to the data server as a root user, and then open a command window. In the following steps, enter commands in the command window that you just opened on the data server.
2. In order to be able to open DB2 Control Center, you must temporarily turn off access control; enter the following command: `xhost +`
3. In DB2 Control Center, view the sample events that are in the sample events table, and obtain the sample event ID numbers:
 - a. To open DB2 Control Center, enter the following commands:

```
su - db2inst1
db2cc
```
 - b. In DB2 Control Center, click **All Databases > IOCDDB > Tables > REF_SAMPLEEVENTS**.
 - c. Right-click the **REF_SAMPLEEVENTS** table, and then click **Open**. There are 40 rows in the sample events table, but, after the events are published, only events 1-8 are displayed in the Details portlet. The other events are for testing KPIs. If you select the **Randomize IDs** check box in the Event Scripting portlet, you can publish the same eight events repeatedly.

- d. Note the **SAMPLEID** for each sample event, to reference when you create event scripts in the Event Scripting portlet. The value of **SAMPLEID** corresponds to the event ID.
4. When you finish viewing the sample events, close DB2 Control Center.
5. To switch back to root user, enter the following command: `exit`
6. To turn access control on again, enter the following command: `xhost -`

Related concepts:

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

Creating an event script

Create an event script that publishes a sequence of events at predefined time intervals.

Before you begin

Before you use the Event Scripting portlet to publish events, you can view the events in the sample events table in the IBM Intelligent Operations Center database.

About this task

Use the following steps to create an event script in the Event Scripting portlet.

Note: You can publish an event with a particular ID only once. To be able to publish an event with the same ID again, click **Reset Database** to delete all the events from the IBM Intelligent Operations Center database. Alternatively, to publish the same events again with random IDs applied, select the **Randomize IDs** check box.

Procedure

1. In the WebSphere Portal Administration interface, click **Intelligent Operations > Demonstration Tools > Event Scripting**.
2. Use the example given in the Event Scripting portlet to create a JSON script that defines a sequential list of events to be published at predefined time intervals; enter the script in the field on the left side of the example. The example JSON script given in the Event Scripting portlet is also shown in the following code:

```
[
  {
    "id": 2
    //ID of element in Sample Events table
    "delayAfter": 4000
    //Milliseconds to wait after publishing the event with the current ID
  },
  {}, //Empty objects are ignored
  {
    "id": 1
    //If the command specifies only an ID, the next command is processed
    //directly after the previous command
  },
  {
    "delayAfter": 0
    //If the command specifies only a delay, no event is published and the
    //script waits until the next command is due
  }
]
```

3. Optional: To publish the same events again with random IDs applied, select the **Randomize IDs** check box.

4. Required: To clean up and validate the script before running it, click **Clean Up and Validate**. The syntax of the script is validated and comments are removed. If incorrect markup is detected in the script that cannot be resolved, a message is displayed.
5. To run the script, click **Run Event Script**.
6. To delete all the events from the IBM Intelligent Operations Center database and prevent the script from publishing any more events, click **Reset Database**.

Related tasks:

“Viewing sample events and KPI events in the sample events table” on page 103

The Event Scripting portlet publishes sample events from the sample events table in the IBM Intelligent Operations Center database. Use the following procedure to view the events in the sample events table.

Creating and integrating KPIs

Key performance indicator (KPI) models can be created and modified using a business monitoring development toolkit and a KPI management portlet.

The IBM WebSphere Business Monitor Development Toolkit can be installed with Rational Application Developer, both are supplied with the IBM Intelligent Operations Center. The IBM WebSphere Business Monitor Development Toolkit can also be installed with WebSphere Integration Developer.

Before defining or modifying a KPI you must understand the Common Alerting Protocol (CAP) alert the KPI will be based on. For example, if you are defining a KPI tracking the level of a water source, you will need to know the CAP elements containing the elements that need to be tracked, such as the name of the water source and the water depth in feet. After a KPI is added or modified in this way it must be deployed to the IBM WebSphere Business Monitor server.

For additional information on using IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit, see the IBM WebSphere Business Monitor information center.

When you have established KPI models and metrics through IBM WebSphere Business Monitor, you can use the Key Performance Indicators portlet to develop and modify KPIs.

Related concepts:

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

“Events and KPIs” on page 87

The IBM Intelligent Operations Center processes events and key performance indicators (KPIs) to determine how information is displayed.

“Customizing KPIs” on page 159

In the IBM Intelligent Operations Center you can customize Key Performance Indicator (KPI) models to suit your business processes.

Related reference:

“Installing tools provided with the solution” on page 62

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

Related information:

 IBM WebSphere Business Process Management Version 7.0 Information Center

Monitor models and KPIs

A monitor model defines metrics and key performance indicators (KPIs), their dependencies on incoming events, conditions requiring business actions, and the outbound events reporting the conditions that might trigger business actions.

A monitor model can contain the following sub-models:

- Monitor details model
- KPI model
- Dimensional model
- Visual model
- Event model

The monitor details model contains most of the monitor model information.

The sample monitor models provided by the IBM Intelligent Operations Center do not use the visual or dimensional models.

The monitor details model defines one or more monitoring contexts. A monitoring context defines the information to be collected and monitored from one or more incoming events. For the IBM Intelligent Operations Center monitored entities are CAP alerts. The information collected from these alerts is used to calculate a KPI.

The KPI model contains one or more KPI contexts. These define the KPIs and their associated triggers and events. KPI contexts can process inbound events, evaluate recurring wait-time triggers and send outbound events. For example, the context can check if a KPI is out of the defined range and send a notification.

The event model refers to all event inbound and outbound definitions used in the monitor model. It refers to schemas describing the structure of individual event parts.

Related concepts:

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

Related information:

IBM Business Monitor information center

Monitoring context instances

A monitoring context instance is information collected at a specific point in time within a monitoring context.

For the IBM Intelligent Operations Center a monitoring context instance corresponds to a CAP alert. When a CAP alert is received, a monitoring context instance is created or reused and the metrics within that context instance are populated with the CAP alert values based on the monitoring context.

A monitoring context can be defined to create a new instance for each CAP alert or to reuse an existing instance. For example, if you want a KPI to calculate the average weekly water level for a given resource with the water level sampled daily, you would create a new monitor context instance for each CAP alert. Each instance would contain the daily water level and the KPI would average the measurements over the seven day period.

KPIs are calculated using the metrics defined for a monitoring context. When defining an aggregation KPI, you specify the monitoring context and metric used as input to the KPI aggregation function. When the KPI is evaluated, the metric values for the monitoring context instances are used by the aggregation function to calculate the KPI value.

Related concepts:

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

Related information:

IBM Business Monitor information center

Modeling KPIs

Model KPIs with Rational Application Developer or WebSphere Integration Developer, with the IBM WebSphere Business Monitor development toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor development toolkit are included as part of the IBM Intelligent Operations Center.

About this task

KPIs are modeled using either Rational Application Developer or WebSphere Integration Developer, with the IBM WebSphere Business Monitor development toolkit. For more information about using these tools, see the information centers for these products.

Monitoring models are contained within business monitoring projects. Models and projects are created using the Rational Application Developer business monitor wizards provided by the IBM WebSphere Business Monitor development toolkit.

To model a KPI, do the following.

Procedure

1. Understand the CAP alert to be received by the IBM Intelligent Operations Center.
2. Understand the purpose of the KPI. Will the KPI generate an action if a limit is reached or exceeded? Will the KPI be used to calculate historical or statistical data?
3. Determine the name for the monitoring context. The IBM Intelligent Operations Center naming convention is to use the CAP event type as the name. The samples provided by IBM Intelligent Operations Center create separate monitoring context for each CAP alert message sent to the IBM WebSphere Business Monitor.
4. In the Rational Application Developer or WebSphere Integration Developer, with the IBM WebSphere Business Monitor development toolkit installed, define the inbound event, key, and set of metrics for the monitor context. The inbound event defines the CAP alert message monitored by the context, a key uniquely defining the context instance, and the metrics defining the information extracted from the CAP alert message.
5. Specify the CAP schema for the event. The schema must exist in the monitoring project. The IBM Intelligent Operations Center provides a copy of the CAP v1.2 schema in the sample `icoc_sample_monitor_models` modeling project.
6. Specify the name and ID for each business monitor inbound event. Event IDs cannot contain spaces or special characters. By default the ID is created from the name with underscores substituted for spaces. All samples provided by the IBM Intelligent Operations Center use default element IDs.
7. Specify the schema. The schema defines the structure of the inbound event to the IBM WebSphere Business Monitor.
8. Define any wanted filtering of CAP messages. For example, limit monitoring to specific event types or severity.
9. Specify the metrics to be extracted from the CAP message.
10. Define a context key to uniquely identify the monitoring context instance. Key values are specified by the inbound event when the monitoring context is created.
11. Specify whether inbound events should be correlated.
12. Specify the KPI context. A KPI context is a container for KPIs and their associated triggers and events. Unlike a monitoring context, a KPI context contains no keys or metrics. A KPI context must be created as a container before creating any KPIs.
13. Create the KPI within the previously defined KPI context.
14. Specify the type of KPI: **Decimal** or **Duration**.
15. Define the KPI ranges, values, and color indicators. Most of the sample IBM Intelligent Operations Center KPIs define three ranges and associated colors.

Table 34. Sample KPI range and color definitions

| Name | Color | RGB |
|-------------|--------|--------|
| Acceptable | green | 699037 |
| Caution | yellow | FDBA1A |
| Take action | red | C32E14 |

16. Define how the KPI value is calculated. KPI values are determined in one of two ways. If the value comes from a metric using an aggregation function, the KPI is referred to as an aggregate KPI. If the value is calculated based on other KPIs or user-defined XPath functions, the KPI is referred to as an expression KPI.

In the IBM Intelligent Operations Center samples, the lowest level KPIs (those KPIs without children) are defined as aggregate KPIs. The higher level KPIs (KPIs with children) are defined as expression KPIs.

Aggregate KPI values are calculated from metrics populated with data sent in CAP alert messages sent to the IBM WebSphere Business Monitor server. An aggregation function is then run on this data. Aggregation functions include:

- average
- maximum
- minimum
- sum
- number of occurrences
- standard deviation

The values are expressed as quantifiable measurements. For example, average crime response time (5 minutes, 7 seconds) or average water level (100.5).

Expression KPI values are calculated from KPI ranges and calculations. In the IBM Intelligent Operations Center samples, the parent KPIs have calculations causing the KPI to evaluate to a value of 0, 1, or 2 depending on the values of their child KPIs. A value of 0 maps to the acceptable range, 1 to the caution range, and 2 to the take action range. The samples use calculation expressions to set the KPI value to the highest urgency of its children.

17. Optional: Specify the time filter for an aggregate KPI. Aggregation KPIs can have optional time filters limiting the period of time over which the KPI value is calculated. The time period can be a repeating interval (for example, the last completed or current period), a rolling interval, or a fixed interval. All sample IBM Intelligent Operations Center aggregate KPIs have defined time filters.
18. Optional: Specify a data filter for the KPI. For example, if the average crime response time is to be calculated for Police Precinct One and no other precinct, a data filter can be used to remove all other monitoring contexts.
19. Define how the KPI values are updated including triggers, events inbound to the IBM WebSphere Business Monitor server and outbound events to the IBM Intelligent Operations Center.
20. Test the KPI. IBM WebSphere Business Monitor development toolkit has a test environment for testing the KPIs prior to deployment, for details see the link at the end of the topic.
21. Deploy the monitor model application.

Related concepts:

“Defining KPI hierarchies”

You can define parent-child relationships between KPIs and design how KPIs are displayed in the IBM Intelligent Operations Center. Design your own KPI hierarchies so that you can look up KPIs in a way that suits your business process.

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

“KPI event communication between IBM WebSphere Business Monitor and IBM Intelligent Operations Center” on page 112

IBM WebSphere Business Monitor can send outbound events from a monitoring or key performance indicator (KPI) context to IBM Intelligent Operations Center.

Related tasks:

“Deploying monitor models” on page 115

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center application server.

Related reference:

“Installing tools provided with the solution” on page 62

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

Related information:

 [Rational Application Developer information center](#)

 [IBM Business Monitor information center](#)

 [XML Path Language \(XPath\) 2.0 \(Second Edition\)](#)

Defining KPI hierarchies

You can define parent-child relationships between KPIs and design how KPIs are displayed in the IBM Intelligent Operations Center. Design your own KPI hierarchies so that you can look up KPIs in a way that suits your business process.

While IBM WebSphere Business Monitor allows a KPI based on the value of another KPI, it does not allow the definition of a parent-child relationship between KPIs. To simplify this task, the IBM Intelligent Operations Center provides a Key Performance Indicators portlet for the administrator. For information about this portlet, see the link at the end of this topic.

The IBM Intelligent Operations Center sample KPIs define a series of Police Department KPIs with a hierarchical design as follows:

```
Police Department ----- level 1
  Crime Response Time ----- level 2
    Crime Response Time Precinct One ----- level 3
    Crime Response Time Precinct Two ----- level 3
```

In this case Police Department has one child: Crime Response Time. Crime Response Time has two children: Crime Response Time Precinct One and Crime Response Time Precinct Two.

The two level 3 KPIs are defined in the KPI model as aggregate KPIs. That is, their values are calculated using a metric value and an aggregation function. All other KPIs in this set are expression KPIs with their values calculated from the values of the other KPIs. For example:

- Crime Response Time is based on the values of Crime Response Time Precinct One and Crime Response Time Precinct Two.
- Police Department is based on the value of Crime Response Time.

The IBM Intelligent Operations Center supports an alternative to the use of the Key Performance Indicators portlet for defining KPI relationships. The Key Performance Indicators portlet is the default method with the **UseDBModelReader** parameter set to true in the system properties table. For information about changing the setting in the system properties table, click the link at the end of this topic. For information about the alternative method for defining KPI relationships, click the link at the end of this topic.

Related concepts:

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

“Defining KPI hierarchies with OWL”

The IBM Intelligent Operations Center supports the use of OWL (Web Ontology Language), as an alternative to the use of the Key Performance Indicators portlet, for defining KPI parent-child relationships.

Defining KPI hierarchies with OWL

The IBM Intelligent Operations Center supports the use of OWL (Web Ontology Language), as an alternative to the use of the Key Performance Indicators portlet, for defining KPI parent-child relationships.

KPI parent-child relationships can be defined in OWL which is read and processed by the IBM Intelligent Operations Center. The definitions are stored in an RDF (Resource Description Framework) file.

You can specify whether or not the KPI database model should be read from an RDF file. For more information on how to change this property in the system properties table, see the link at the end of this topic.

An example of the OWL definitions for the Police Department sample KPI set is as follows:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
  rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
```

```
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

Note: OWL is a language built on RDF. OWL and RDF are similar, but OWL is a stronger language. OWL provides a larger vocabulary, stronger syntax, and greater machine interpretability than RDF.

Related concepts:

“Defining KPI hierarchies” on page 110

You can define parent-child relationships between KPIs and design how KPIs are displayed in the IBM Intelligent Operations Center. Design your own KPI hierarchies so that you can look up KPIs in a way that suits your business process.

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

KPI event communication between IBM WebSphere Business Monitor and IBM Intelligent Operations Center

IBM WebSphere Business Monitor can send outbound events from a monitoring or key performance indicator (KPI) context to IBM Intelligent Operations Center.

Outbound events from the IBM WebSphere Business Monitor server are placed on an external message queue. The IBM Intelligent Operations Center uses this mechanism to asynchronously receive KPI updates.

Note: You can specify whether or not the connection to IBM WebSphere Business Monitor is to use SSL for secure connection. For more information on how to change this property in the system properties table, see the link at the end of this topic.

Related concepts:

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

“Using the inbound event queue defined for the IBM Intelligent Operations Center” on page 95

CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

Triggers

A trigger is a mechanism that detects an occurrence and can cause additional processing in response to that occurrence.

The KPI samples provided with the IBM Intelligent Operations Center define two types of triggers. The first trigger is fired when a CAP alert message, also known as an inbound event, is received by the IBM WebSphere Business Monitor server for a defined KPI set. The CAP alert message might, or might not, change the KPI. The IBM Intelligent Operations Center determines if the KPI is changed when it receives the event notification from the IBM WebSphere Business Monitor server.

For outbound events, a trigger determines when the event will be sent.

Event based triggers can be used to send notifications to the IBM Intelligent Operations Center when input for a KPI calculation changes. However, event triggers cannot be used to address the situation

when a KPI value changes after a defined time period expires. In the IBM Intelligent Operations Center samples, time based triggers are used to send notifications to the IBM Intelligent Operations Center for those KPIs with short time period definitions.

For example, the Severe Traffic Accidents KPI is defined to expire every hour. If the KPI has a value of 3 at 10:00 and no CAP alert messages are received for that KPI during the next hour, then the time period expires and the KPI value is reset to 0.

Defining inbound events to IBM WebSphere Business Monitor

In the IBM Intelligent Operations Center samples, inbound events are used to determine when a trigger is fired. Inbound events for a KPI context are defined in a similar manner to those for a monitoring context.

About this task

Inbound events are defined using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor development toolkit. For more information on using these tools, see the information centers for these products.

To define an inbound event, do the following.

Procedure

1. Select the KPI context for the inbound event.
2. Create the inbound event and specify the event name and ID.
3. Specify the CAP schema.
4. Specify the filter condition.
5. Select the KPI context and create a new inbound event.
6. Create a new trigger for the inbound event.
7. Make sure that the trigger is repeatable so the trigger fires each time the trigger source is updated and the trigger condition is met.
8. Select the trigger source.
9. Define the trigger condition. When the trigger condition is met, the trigger fires.

Example

The sample IBM Intelligent Operations Center monitor models are defined so that a trigger fires each time a CAP alert message is received by the IBM WebSphere Business Monitor server.

Related tasks:

“Modeling KPIs” on page 107

Model KPIs with Rational Application Developer or WebSphere Integration Developer, with the IBM WebSphere Business Monitor development toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor development toolkit are included as part of the IBM Intelligent Operations Center.

Related information:

 IBM Business Monitor information center

 Rational Application Developer information center

Defining outbound events to the IBM Intelligent Operations Center

Outbound events define the information sent from the IBM WebSphere Business Monitor to the IBM Intelligent Operations Center when a trigger fires.

About this task

The IBM Intelligent Operations Center uses outbound notifications sent from the IBM WebSphere Business Monitor server to determine if the KPI has changed. If the KPI has changed, the IBM Intelligent Operations Center obtains the KPI data from the IBM WebSphere Business Monitor server, updates the KPI cache information, and updates the IBM Intelligent Operations Center data.

Outbound events are defined using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor development toolkit. For more information on using these tools, see the information centers for these products.

To define an outbound event, do the following steps.

Procedure

1. Select the KPI context for the outbound event.
2. Create the outbound event and specify the event name and ID.
3. Specify the notification schema. The schema is located in the `ioc-notification-v1.0.xsd` file. The schema is located in the `icoc_sample_monitor-models` project.
4. Define the content of the outbound event. The content is based on the notification schema.
5. Under **notification**, for the value of **sentfrom** enter Monitor.
6. Add the parameter elements to the event content, as defined in the following substeps:
 - a. For the first parameter, specify `modelId` for **parameterName** and the monitor model ID for **parameterValue**. For example, `icoc_sample_public_safety_monitor_model`.
 - b. For each KPI in the KPI set, add parameters to specify the KPI ID and KPI value. The KPI ID is specified using the **parameterName** element and the KPI value is specified using the **parameterValue** element. The KPI ID must be associated with a KPI in the KPI set. Use the `xs:string()` function to specify the KPI value as a string. For example, **parameterName** can be `Police_Department` and **parameterValue** can be `xs:string(Police_Department)`.

Example

The following is an example of a notification to be sent to the IBM Intelligent Operations Center:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
  <ns1:parameter>
    <ns1:parameterName> modelId</ns1:parameterName>
    <ns1:parameterValue>
      icoc_sample_public_safety_monitor_model</ns1:parameterValue>
    </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Police_Department</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
  </ns1:parameter>
</ns1:notification>
```

```
<ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
<ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
</ns1:parameter>
</ns1:notification>
```

Related tasks:

“Modeling KPIs” on page 107

Model KPIs with Rational Application Developer or WebSphere Integration Developer, with the IBM WebSphere Business Monitor development toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor development toolkit are included as part of the IBM Intelligent Operations Center.

Related information:

 [IBM Business Monitor information center](#)

 [Rational Application Developer information center](#)

Deploying monitor models

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center application server.

About this task

To deploy a monitor model that will be used by the IBM WebSphere Business Monitor, Java Enterprise Edition (JEE) projects must be generated from the defined models. Once the JEE projects are generated, the model application can be exported as an EAR file. The EAR file can then be deployed into the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center application server.

Procedure

1. In Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor development toolkit installed, right-click the monitor model requiring project generation in the **Enterprise Explorer** tab. For example, `icoc_sample_public_safety_monitor_model`.
2. Click **Generate Monitor JEE Projects**. The following projects will be created: `modelApplication`, `modelLogic`, and `modelModerator`.
3. Export the monitor model application by right-clicking the `modelApplication` project and clicking **Export > EAR**.
4. Test the KPIs before deploying the EAR file into IBM WebSphere Business Monitor.
5. Deploy the EAR file into the IBM WebSphere Business Monitor server using the instructions in the IBM WebSphere Business Monitor information center.

Related information:

 [IBM Business Monitor information center](#)

 [Rational Application Developer information center](#)

KPI display values

The IBM Intelligent Operations Center resource bundles can be used to provide alternate display values from those values provided by the IBM WebSphere Business Monitor models.

KPI display names and range names are defined in the sample IBM WebSphere Business Monitor models provided with the IBM Intelligent Operations Center. Examples of KPI display names are:

- Water
- Water Quality

Examples of range names are:

- acceptable status value
- caution status value
- take action status value

Each artifact, for example KPI and range, defined in IBM WebSphere Business Monitor has an ID associated with the display name. IDs cannot contain spaces while display values can. The IDs are used as keys to look up values in a resource bundle. The IBM Intelligent Operations Center uses these IDs to select KPI display values. If no values are specified in the resource bundle for the ID, the value specified in the IBM WebSphere Business Monitor definition are used.

The KPI display values are localized by IBM WebSphere Business Monitor using the ISO language and country codes of the IBM WebSphere Business Monitor server. For example, a KPI percentage value would be displayed in the format 12.61% when the locale is en_US and 12,61% when the locale is fr_FR. Resource bundle definitions are not used for these values.

The default IBM Intelligent Operations Center properties resource bundle is `com.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. The bundle can be found in `icoc_rest_monitor_resources_utils`.

This is an example resource bundle:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

In this example, the values of `kpi.NO.VALUE` and `kpi.RANGE.UNDETERMINED` are used by the IBM Intelligent Operations Center when the IBM WebSphere Business Monitor KPIs return a null value. For example, the Water Level City Lake KPI is defined with a repeating daily time period based on the last full period. If no CAP events are received for that KPI on a Sunday, and the KPI is requested on Monday, null is returned since no data is available for the previous day. The display value is set to "No data to determine the KPI value" and the range display name is set to "undetermined".

The other entries, `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River`, and `Water_Level_City_Lake`, define the display values for the KPI IDs defined in the `icoc sample water monitor model sample monitor model` provided by the IBM Intelligent Operations Center. These entries can specify alternate text from the values specified in the IBM WebSphere Business Monitor monitor. For example, the resource bundle can be used to provide translated values instead of changing the model itself.

Related concepts:

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

Caching KPIs

IBM Intelligent Operations Center configuration settings affect when KPI values are retrieved from the IBM WebSphere Business Monitor.

The IBM Intelligent Operations Center maintains KPI values in a cache. By default, the KPIs are loaded from IBM WebSphere Business Monitor into the cache and the cache is refreshed according to the time interval specified by `KpiCacheRefreshInterval` property in the system properties table. This refresh time

can be altered depending on your requirements to deliver updated KPIs to the IBM Intelligent Operations Center. For more information on changing properties in the system properties table, see the link at the end of the topic.

Note that when you create a KPI in the Key Performance Indicators portlet, updates to the KPI depend solely on the cache refresh. When a KPI is defined in IBM WebSphere Business Monitor, a trigger mechanism can be defined to implement additional processing in response to changes in that KPI.

Related concepts:

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

Sample KPIs

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

The lowest level KPIs are defined as aggregate KPIs. Aggregate KPIs are calculated from values contained in incoming CAP alert messages and an aggregation function such as average, maximum, minimum, sum, number of occurrences, or standard deviation. Their values are expressed as quantifiable measurements. Lower level KPI values are localized into the appropriate format based on the locale of the IBM WebSphere Business Monitor server. The higher level KPIs are mapped to values based on the mapping defined when the sample KPI was created.

The value of the higher level sample KPI is a number which equates to color and the level of response recommended. A value of 0 is acceptable, a value of 1 is caution, and a value of 2 is take action. The value of the lowest level KPI is a duration, a decimal, a percentage or a currency depending on the KPI it represents. For example:

- 15% is the actual value of a KPI representing the percentage of delayed flights at a particular airport over a period of time.
- 5 minutes, 7 seconds is the actual value of a KPI representing the average crime response time for a given location over a period of time.

The source files for the sample IBM Intelligent Operations Center monitor models are provided in an archive file that can be imported into Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Toolkit installed. The archive file can be modified to change, add, or delete KPI definitions. The definitions can then be regenerated and redeployed to the IBM Intelligent Operations Center.

The sample models shipped with the IBM Intelligent Operations Center are:

- `icoc_sample_public_safety_monitor_model`
- `icoc_sample_transportation_monitor_model`
- `icoc_sample_water_monitor_model`

These models contain the following KPI samples:

- Water
 - Flood Control
 - Water Levels
 - Flow Discharge City River
 - Water Level City Lake
 - Water Management

- Strategical Planning
 - Water Leakage
 - Water Supply vs Demand
- Water Quality
 - Physical Indicators
 - Turbidity
 - pH
- Transportation
 - Airports
 - Delayed Flights
 - Delayed Flights Airport One
 - Delayed Flights Airport Two
 - Roads and Traffic
 - Road Events
 - Severe Traffic Accidents
 - Transportation Management
 - Revenue
 - Bridges and Tunnel Tolls
 - Parking Facilities Revenue
- Public Safety
 - Fire Department
 - Firefighter Injuries
 - Firefighter Injuries Fire Station One
 - Firefighter Injuries Fire Station two
 - Police Department
 - Crime Response Time
 - Crime Response Time Precinct One
 - Crime Response Time Precinct Two
 - Public Safety Management
 - Public Safety Budget
 - EMS Department Budget
 - Fire Department Budget
 - Police Department Budget

Related concepts:

“Status” on page 274

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

“Key Performance Indicator Drill Down” on page 260

Use the Key Performance Indicator Drill Down portlet to see more information about a KPI category, the status of its underlying KPIs.

“Creating and integrating KPIs” on page 105

Key performance indicator (KPI) models can be created and modified using a business monitoring development toolkit and a KPI management portlet.

“Customizing KPIs” on page 159

In the IBM Intelligent Operations Center you can customize Key Performance Indicator (KPI) models to suit your business processes.

Related tasks:

“Deploying monitor models” on page 115

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center application server.

“Viewing sample events and KPI events in the sample events table” on page 103

The Event Scripting portlet publishes sample events from the sample events table in the IBM Intelligent Operations Center database. Use the following procedure to view the events in the sample events table.

Configuring Tivoli Service Request Manager

In the Tivoli Service Request Manager user interface, you can manage standard operating procedures, workflows, and resources.

If you add a common prefix to the names of standard operating procedures, workflows, and resources, it is easier to filter the data in a search. For example, for customer projects, use the common prefix CX.

You can specify whether the connection to Tivoli Service Request Manager uses SSL by setting the **TSRMServerSecurityEnabled** property. For more information about this property and other Tivoli Service Request Manager properties, go to the link at the end of the topic.

Related concepts:

“Event server” on page 196

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

Using the Tivoli Service Request Manager user interface

Learn how to access the Tivoli Service Request Manager user interface. Make the Tivoli Service Request Manager Start Center easier and faster to use by customizing it with links to the features that you use most.

Opening Tivoli Service Request Manager applications

You can open Tivoli Service Request Manager applications through the WebSphere Portal Administration interface, either through Solution Administration Tools, or through the Standard Operating Procedures portlet. You can also view a resource in Tivoli Service Request Manager through the IBM Intelligent Operations Center interface.

Before you begin

To be able to view a resource in Tivoli Service Request Manager through the IBM Intelligent Operations Center interface, single sign-on must be configured.

Procedure

- To open the Tivoli Service Request Manager Start Center through the WebSphere Portal Administration interface, use the following substeps:
 1. Click **Intelligent Operations > Administration Tools > Administration Consoles**.
 2. Click **Standard Operating Procedure Administration**.
 3. Log on to the Tivoli Service Request Manager Start Center as an administrator.
- To open Tivoli Service Request Manager applications related to standard operating procedures, use the Standard Operating Procedures portlet:
 1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
 2. Choose one of the following options:
 - To open the Standard Operating Procedure application, click **Standard Operating Procedures**.
 - To open the Standard Operating Procedure Selection Matrix application, click **Standard Operating Procedures Selection Matrix**.
 - To open the workflow designer application, click **Workflow Designer**.
- To view a resource in the Tivoli Service Request Manager user interface through the IBM Intelligent Operations Center interface, do the following steps:
 1. In the Details portlet, on the **Events and Incidents** tab, right-click a row in the events list.
 2. To view a list of the resources in the vicinity of the event, click **View Nearby Resources** and select the radius of the area you want to focus on. A list of resources is displayed on the **Resources** tab.
 3. On the **Resources** tab, right-click a row in the resources list, and then click **Properties**. The resource is displayed in Tivoli Service Request Manager, on the **Resources** tab.

Note: To completely sign out of Tivoli Service Request Manager, you must close the Tivoli Service Request Manager user interface web browser window.

Related tasks:

“Configuring single sign-on for collaboration services” on page 50

Import the WebSphere Portal SSO LTPA token into the event server to allow users to access collaboration services without having to reenter their credentials.

Setting up favorite applications in the Tivoli Service Request Manager Start Center

Update your favorite applications in the Tivoli Service Request Manager Start Center so that you can access them more easily.

About this task

Each Tivoli Service Request Manager user has their own Tivoli Service Request Manager Start Center with the user's own customized list under Favorite Applications.

Procedure

1. To view the Tivoli Service Request Manager Start Center, at the top of the Tivoli Service Request Manager user interface, click **Start Center**.
2. In the Tivoli Service Request Manager Start Center, click the **Edit Portlet** icon next to Favorite Applications.
3. In the Favorite Applications Setup window, click **Select Applications**.

4. In the Select Applications window, select the applications that you want to be displayed under Favorite Applications. The following list shows applications that are useful to IBM Intelligent Operations Center users:

CRONTASK

Cron Task Setup

DOMAINADM

Domains

PERSON

People

PERSONGR

Person Groups

PLUSIMTRIX

SOP Selection Matrix

PLUSIRES

Resources

PLUSIWO

SOP Activities

USER Users

WFDESIGN

Workflow Designer

5. To define the position in which applications are listed under Favorite Applications, do the following steps:
 - a. In the Favorite Applications Setup window, select an application.
 - b. In the **Order** field, enter a number.
6. To save the updates, click **Finished**.

Configuring new users in Tivoli Service Request Manager

When you add a user in IBM Intelligent Operations Center, assign permissions and person groups for the user in Tivoli Service Request Manager.

Setting the Default Insert Site

For a new user to be able to add new resources and apply standard operating procedures, you must set the Default Insert Site for the user.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go To > Security > Users**.
3. To search for the user, on the **List** tab, in the **User** field, enter some or all of the letters in the name of the user.
4. In the list, click the name of the user, and then click the **User** tab.
5. Under User Settings, next to the **Default Insert Site** field, click the **Select Value** icon.
6. In the Select Value window, search for and click the name of the Default Insert Site; for example, **PMSCRTP**. PMSCRTP is a sample site that is installed with the IBM Intelligent Operations Center.
7. Click the **Save User** icon.

Assigning a user to a security group

Add users to the appropriate security groups, so that they have access to the appropriate applications in Tivoli Service Request Manager.

About this task

To add a user to a group, use the following procedure.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go To > Security > Users**.
3. To search for the user, on the **List** tab, in the **User** field, enter some or all of the letters in the name of the user.
4. In the list, click the name of the user, and then click the **Groups** tab.
5. To search for the group that you want to add the user to, in the **Group** field, enter some or all of the letters in the name of the group.
6. If the name of the required group is not listed, click **New Row**.
7. Under Details, next to the **Group** field, click the **Detail Menu** icon, and then click **Select Value**.
8. In the Select Value window, search for and click the name of the required group.
9. Click the **Save User** icon.

Assigning a user to a person group

In a standard operating procedure, the tasks can be assigned to predefined person groups. A user must be a member of a particular person group in order to see the tasks assigned to that person group.

Before you begin

You can either use the sample person groups provided during the installation of IBM Intelligent Operations Center, or you can create your own person groups. For information on how to create a person group in Tivoli Service Request Manager, see the Maximo® Asset Management information center.

Note: Ensure that the names of all the person groups are the same length. This ensures that users are assigned only tasks that are allocated to the person groups of which they are members.

About this task

To assign a user to a person group, use the following procedure.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go To > Administration > Resources > Person Groups**.
3. To search for the required person group, on the **List** tab, in the **Person Groups** field, enter some or all of the letters in the name of the person group.
4. In the list, click the name of the person group.
5. On the **Person Group** tab, under People, click **New Row**.
6. Under Details, next to the **Person** field, click the **Detail Menu** icon, and then click **Select Value**.
7. In the Select Value window, search for and click the name of the user you want to add to the person group.
8. In the **Sequence** field, enter the next available incremental number.
9. Click the **Save Person Group** icon.

Related information:

 [Maximo Asset Management information center](#)

Standard Operating Procedures

You can define standard operating procedures and activities to manage events that come into the IBM Intelligent Operations Center. Use the Standard Operating Procedures portlet to access the standard operating procedure, standard operating procedure selection matrix, and workflow designer applications in Tivoli Service Request Manager.

To launch the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.

A standard operating procedure defines a sequence of activities that are triggered in response to an event whose parameters meet certain predefined conditions, where each activity corresponds to either a manual or an automated task. You can assign a workflow to an automated task. Each activity is assigned to an owner group, and users are assigned to an owner group through their membership of a person group. All users who are assigned to the owner group can manage the activities through the My Activities portlet.

You can specify the order in which some or all of the activities in a standard operating procedure are executed. For example, you can specify that a particular activity is not started until the previous activity is completed or skipped.

To open the standard operating procedure application, in the Standard Operating Procedures portlet, click **Standard Operating Procedures**.

Standard operating procedure selection matrix

In the standard operating procedure selection matrix, you define the event parameters that determine whether a standard operating procedure is initiated for a particular event. Each standard operating procedure can have one or more sets of selection criteria. However, each set of selection criteria must be unique.

To open the standard operating procedure selection matrix application, in the Standard Operating Procedures portlet, click **Standard Operating Procedures Selection Matrix**.

Workflow designer

Use the workflow designer to design workflows that can be assigned to your standard operating procedure activities as automated tasks.

To open the workflow designer application, in the Standard Operating Procedures portlet, click **Workflow Designer**.

Customizing the Standard Operating Procedures portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related concepts:

“My Activities” on page 269

The My Activities portlet displays a dynamic list of activities that are owned by the group of which the user, who is logged on to the interface, is a member.

Related reference:

“Standard Operating Procedures portlet settings” on page 156

Customize the Standard Operating Procedures portlet by changing the settings in the fields of the **Shared Settings** window.

Creating workflows

In Tivoli Service Request Manager, you can create workflows that you can include as automated tasks in your standard operating procedure activities.

About this task

For detailed information about how to create workflows, see the link to the Maximo Asset Management information center at the end of the topic.

Procedure

1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
2. To open the workflow designer application, click **Workflow Designer**.
3. In the Workflow Designer window, click the **Canvas** tab.
4. On the **Canvas** tab, click the appropriate icons to insert the required nodes and arrows for the workflow.

Related information:

 [Maximo Asset Management information center](#)

Creating standard operating procedures

Create a standard operating procedure, and assign it to an owner group. Users are assigned to an owner group through their membership of a person group.

Procedure

1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
2. To open the standard operating procedure application, click **Standard Operating Procedures**.
3. In the Standard Operating Procedure window, on the **List** tab, click the **New SOP** icon. A blank standard operating procedure is displayed on the **Standard Operating Procedure** tab.
4. For **SOP Name**, enter a name, and in the field next to **SOP Name**, enter a description. For the names of standard operating procedures, use a consistent format that is similar to the names of the sample standard operating procedures; for example, Prepare for severe weather evacuation (Prepare). Also, if the last character of the name is a closing parenthesis, append the left-to-right mark (LRM) character to prevent potential problems related to the rendering of bidirectional text. For example, enter the name used in the previous example as Prepare for severe weather evacuation (Prepare)‎. The LRM character is not displayed in the user interface after you save the standard operating procedure. Also, if you add a common prefix to the names of all your standard operating procedures, it is easier to filter your standard operating procedures in a search. For example, for customer projects, use the common prefix CX.
5. To enter a longer description, click the icon next to the description field and enter a description in the window that is displayed.
6. Under Details, from the **Template Type** list, select **Activity**.

7. Under Details, assign an owner group to the standard operating procedure:
 - a. Click the icon next to the **Owner Group** field.
 - b. In the Select Value window, click a value in the list to select it.
8. Optional: For **Duration**, enter a time limit that the standard operating procedure must be completed in. The format for the time limit is *hh:mm*, where *hh* is the number of hours and *mm* is the number of minutes. The due date is calculated based on the duration.
9. Add tasks to the standard operating procedure, as required:
 - a. Near the lower right of the Tivoli Service Request Manager user interface, click **New Row**. Under SOP Steps, a new task row is appended to the task sequence list.
 - b. For **Sequence**, and for **Task**, enter the same number. Number tasks with the following pattern: 10, 20, 30, and so on. If you use this pattern, you have more flexibility to add and remove tasks later.
 - c. For **Instruction**, enter a task description. To select from descriptions that you have entered previously, click the icon next to the description field.
 - d. Optional: Assign a workflow:
 - 1) For **Workflow Name**, click the **Select Value** icon.
 - 2) In the **Select Value** window, click a value in the list to select it. To narrow down the list, in the filter field that is displayed at the top of the list, enter the first few letters of the name of a workflow that you want to use.
 - 3) Expand the task row and, under Details, enter more details as required. If you want, you can specify an owner group, and flow control settings. If you do not specify an owner group and flow control settings for the task, the task inherits the settings from the parent standard operating procedure.
10. To save the standard operating procedure, near the top of the Tivoli Service Request Manager user interface, click the **Save SOP** icon.
11. For the standard operating procedure to be applied to the events specified in the standard operating procedure selection matrix, ensure that you change the status from DRAFT to ACTIVE:
 - a. Click the **Change Status** icon.
 - b. In the Change Status window, from the **New Status** list, select **Active**.
 - c. Optional: Enter values for **As Of Date** and **Memo**.
 - d. Click **OK**.
12. To review the available standard operating procedures, do the following steps:
 - a. Click the **List** tab.
 - b. Under SOP Job Plans, choose one of the following options:
 - In the filter field, press Enter to view all the available standard operating procedures.
 - In the filter field, enter the first few letters of the name of a standard operating procedure.
 - c. To view the details for a standard operating procedure, click the name of the standard operating procedure in the list. The details are displayed on the **Standard Operating Procedure** tab.

What to do next

If you want to be able to specify the order in which some or all of the activities in a standard operating procedure are executed, under Details, select the **Flow Controlled?** check box. For more information about how to order the activities that are assigned to users or groups based on standard operating procedures, see the Maximo Asset Management information center and search for *flow control*.

In the standard operating procedure selection matrix, define the event parameters that determine for which events the standard operating procedure is selected.

Related tasks:

“Assigning a user to a person group” on page 122

In a standard operating procedure, the tasks can be assigned to predefined person groups. A user must be a member of a particular person group in order to see the tasks assigned to that person group.

Related information:

 [Maximo Asset Management information center](#)

Reviewing entries in the standard operating procedure selection matrix

In the standard operating procedure selection matrix, review the selection criteria for each standard operating procedure. The selection criteria are based on event parameters.

Procedure

1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
2. To open the Standard Operating Procedure Selection Matrix application, click **Standard Operating Procedures Selection Matrix**.
3. In the Standard Operating Procedure Selection Matrix window, to display the filter row, click the **Filter** icon.
4. Determine which filter field to use:
 - Category
 - Severity
 - Urgency
 - Certainty
 - SOP Name
5. Choose one of the following options:
 - In the filter field, press Enter to view all the existing entries that relate to your chosen parameter or standard operating procedure name.
 - In the filter field, enter the first few letters of a value to filter on.
 - If you are filtering on a parameter value, enter values through the Select Value window:
 - a. Next to the filter field, click the **Select Value** icon.
 - b. In the Select Value window, click a value in the list to select it.
 - To select the name of a standard operating procedure to filter on through the Standard Operating Procedure window:
 - a. Next to the **SOP NAME** filter field, click the **Detail Menu** icon, and then click **Go To Standard Operating Procedure**.
 - b. In the Standard Operating Procedure window, click the **List** tab.
 - c. Under SOP Job Plans, in the filter field, enter the first few letters of the name of a standard operating procedure.
 - d. To view the details for a standard operating procedure, click the name of the standard operating procedure in the list. The details are displayed on the **Standard Operating Procedure** tab.
 - e. To return the name of the standard operating procedure that is displayed on the **Standard Operating Procedure** tab, in the upper right corner, click **Return With Value**. The name is displayed in the **SOP Name** filter field in the selection matrix.
6. To further refine the list of displayed selection criteria entries, repeat Step 5 using one of the other filter fields listed in Step 4.

Defining parameters in the standard operating procedure selection matrix

In the standard operating procedure selection matrix, define the event parameters that determine whether a standard operating procedure is selected for a particular event.

About this task

You cannot save a standard operating procedure selection matrix that contains two rows of identical selection criteria. If appropriate, a validation message is displayed that informs you that you must define a unique set of selection criteria for a standard operating procedure.

Procedure

1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
2. To open the Standard Operating Procedure Selection Matrix application, click **Standard Operating Procedures Selection Matrix**.
3. In the Standard Operating Procedure Selection Matrix window, to display the filter row, click the **Filter** icon.
4. In the **SOP Selection Matrix** window, in the lower right corner, click **New Row**. A new row is appended to the selection matrix.
5. Enter values for each of the following parameters:
 - Category
 - Severity
 - Urgency
 - Certainty

Use one of the following options to enter values for each of the parameters:

- To enter values through the Select Value window:
 - a. Next to the parameter field, click the **Select Value** icon.
 - b. In the Select Value window, click a value in the list to select it.
 - To enter the name of the parameter manually:
 - a. Enter the first few letters of the value of the parameter in the field.
 - b. Press the TAB key to move the cursor to the next field, and the value of the parameter is automatically completed.
6. To enter the name of the standard operating procedure in the **SOP Name** field, choose one of the following options:
 - To enter the name of the standard operating procedure through the Standard Operating Procedure window:
 - a. Next to the **SOP NAME** field, click the **Detail Menu** icon, and then click **Go To Standard Operating Procedure**.
 - b. In the Standard Operating Procedure window, click the **List** tab.
 - c. Under SOP Job Plans, in the filter field, enter the first few letters of the name of a standard operating procedure.
 - d. To view the details for a standard operating procedure, click the name of the standard operating procedure in the list. The details are displayed on the **Standard Operating Procedure** tab.
 - e. To return the name of the standard operating procedure that is displayed on the **Standard Operating Procedure** tab, in the upper right corner, click **Return With Value**. The name is displayed in the **SOP Name** field of the new row in the selection matrix.
 - Enter the name of the standard operating procedure manually.
 7. Click the **Save matrix** icon.

Managing resources

Manage your resources in Tivoli Service Request Manager.

Synchronizing the sample resources to the IBM Intelligent Operations Center database

If you want to use the sample resources that are installed with IBM Intelligent Operations Center, you must synchronize them to the IBM Intelligent Operations Center database manually.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go to > Assets > IOC Resources (IntOpCtr)**.
3. To view all the sample IBM Intelligent Operations Center resources, in the Resources (IntOpCtr) window, on the **List** tab, click the **Resource** field, and then press Enter.
4. For each resource that you want to synchronize to the IBM Intelligent Operations Center database, update the resource. For example, modify the **Description** and save the change.
5. Verify that the synchronized resources are listed in the following IBM Intelligent Operations Center database tables:
 - IOC.RESOURCE
 - IOC.RESOURCE_X_CAPABILITY

What to do next

If the sample resources are not correctly synchronized to the IBM Intelligent Operations Center database, review the Tivoli Netcool/Impact probe log file. Enter the following command:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Also, review the Tivoli Netcool/Impact policy log file at `/opt/IBM/netcool/impact/log/NCI_policylogger.log`. To enable the Tivoli Netcool/Impact policy log file, do the following steps:

1. Log on to the Tivoli Netcool/Impact administrative console at `http://event_server:9080/nci`. Log on as the admin user with the netcool password.
2. Click **IOC Project**.
3. On the **Services** tab, click **Policy Logger**.
4. For **Highest Level Log**, change the value from 0 to 3.
5. Save the changes.
6. Run the test.

For more information about troubleshooting log files, see the link at the end of the topic.

Related concepts:

“Event server log files” on page 280

Use the following procedures to enable traces and view logs for some of the systems on the event server.

Creating or modifying the event category to capability mapping

Resources are displayed on the Map portlet depending on the category of the selected event and the mapped resource capabilities. Before you create a resource, map the capability of the resource to the appropriate event category.

Before you begin

To ensure that the resource capabilities are updated, you must set the value of the password for the Tivoli Service Request Manager administrative user, for example, **maxadmin**, to maxadmin.

About this task

Mapping a resource capability to an event category ensures that, when you view nearby resources in the IBM Intelligent Operations Center Details portlet, the appropriate resources are displayed in the Map

portlet. For example, if you view nearby resources for a meteorological category of event, a warehouse that stores sand bags is displayed, where the warehouse is the resource type and the sandbags are a mapped capability of the warehouse.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go to > System Configuration > Platform Configuration > Domains**.
3. Choose the appropriate option:
 - To create an event category to capability mapping, click **New Row** and enter the appropriate details into the fields.
 - To modify an existing event category to capability mapping, use the filter field to display the appropriate event category mappings, then click the row you want to edit and modify the details.
 - To delete an existing event category to capability mapping, use the filter field to display the appropriate event category mappings, then click the **Mark Row for Delete** icon at the end of the row that you want to delete.
4. Click the **Save Domain** icon.
5. Verify that the mapped resources are listed in the following IBM Intelligent Operations Center database tables:
 - IOC.RESOURCE
 - IOC.RESOURCE_X_CAPABILITY

Results

New resources whose capability is mapped to the event category of the currently selected event are displayed on the IBM Intelligent Operations Center Map portlet immediately. Updated resources whose capability is mapped to the event category of the currently selected event are displayed only after the page containing the IBM Intelligent Operations CenterMap portlet is reloaded.

What to do next

- If the mapped resources are not correctly listed in the IBM Intelligent Operations Center database, review the Tivoli Netcool/Impact log file. Enter the following command:

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

For more information about troubleshooting log files, see the link at the end of the topic.

- If you want to map more than two event categories to a capability, use a DB2 command to do the mapping. Use the following steps:
 1. To log on to the data server as a Tivoli Service Request Manager database user, enter the following command: `su - db2inst6`
 2. To connect to the IBM Intelligent Operations Center database, enter the following command: `db2 connect to maximo`
 3. To map an event category to a capability, enter the following command:

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'category_name', 'capability_name',
'mapping_description', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|mapping_key');
```

In the previous command, replace the variables *category_name*, *capability_name*, *mapping_description*, and *mapping_key* with appropriate values. For *mapping_key*, create an appropriate value. For example, the following command maps the event category Met to the capability COT, and assigns the value METCOT to *mapping_key*.

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|METCOT');
```

4. To complete the write to the database, enter the following command: db2 commit;

Creating a resource

Create a resource in the Tivoli Service Request Manager user interface.

Before you begin

Ensure that the capability of the new resource is mapped to a category so that the resource is displayed on the Map portlet in the IBM Intelligent Operations Center user interface.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go to > Assets > Resources (IntOpCtr)**.
3. In the IOC Resources window, click the **New Resource** icon.
4. On the **Resource** tab, enter the following details:

Resource

A unique ID for the resource.

Long Description

The name of the resource that is displayed in the IBM Intelligent Operations Center user interface, in the Details portlet, on the **Resources** tab.

Short Description

A short description of the resource that is displayed as hover help if you hover over the resource in the Map portlet in the IBM Intelligent Operations Center user interface.

Latitude

The latitudinal position of the location of the resource.

Longitude

The longitudinal position of the location of the resource.

5. Click the **Capabilities** tab.
6. Next to the **Classification** field, click the **Detail Menu** icon, and then click **Classify**.
7. In the Classify window, browse the navigation tree to locate the appropriate resource classification.
8. Click a classification name; for example, a warehouse. A table of capabilities associated with the classification is displayed in the IOC Resources window.
9. In the Capabilities table, click the appropriate capabilities and enter the **Numeric value**.
10. Click the **Save Resource** icon.

What to do next

Verify that the resource is listed in the following IBM Intelligent Operations Center database tables:

- IOC.RESOURCE
- IOC.RESOURCE_X_CAPABILITY

Related tasks:

“Creating or modifying the event category to capability mapping” on page 128

Resources are displayed on the Map portlet depending on the category of the selected event and the mapped resource capabilities. Before you create a resource, map the capability of the resource to the appropriate event category.

Viewing, updating, or deleting a resource

Access the Tivoli Service Request Manager user interface through the IBM Intelligent Operations Center user interface and view, update, or delete your resources.

About this task

The following procedure describes how to access resource data in Tivoli Service Request Manager through the IBM Intelligent Operations Center user interface. To access resource data directly through Tivoli Service Request Manager, use the following steps:

1. Log on to the Tivoli Service Request Manager Start Center.
2. Click **Go to > Assets > Resources (IntOpCtr)**.
3. To list all the IBM Intelligent Operations Center resources, in the Resources (IntOpCtr) window, on the **List** tab, click in the **Resource** field and press the Enter key.
4. In the list, click the row for the resource that you want to modify.
5. Click the **Resource** tab or the **Capabilities** tab, as appropriate.

Procedure

1. Open the IBM Intelligent Operations Center user interface.
2. In the Details portlet, on the **Events and Incidents** tab, identify an event in the list whose resources you want to view, update, or delete.
3. To view a list of the resources in the vicinity of the event, right-click the event, and then click **View Nearby Resources** and select the radius of the area you want to focus on. A list of resources is displayed on the **Resources** tab.
4. On the **Resources** tab, right-click a row in the resources list and select an option from the menu:
 - To update the information about a resource, click **Update**.
 - To remove a resource from the list and the map, click **Delete**.
 - To view the information about a resource, click **Properties**.

Whichever option you choose, the resource is displayed in Tivoli Service Request Manager, on the **Resource** tab.

5. In Tivoli Service Request Manager, on the **Resource** tab, you can choose to do the following actions on the resource:
 - Update the resource name, descriptions, latitude, and longitude.
 - To delete the resource, select **Delete Resource** from the **Select Action** list.
6. On the **Capabilities** tab, you can choose to do the following actions on the resource capabilities.
 - Click the appropriate capabilities and modify the **Numeric value**. For a capability to be mapped to the resource, the value must be 1 or more.
 - Select a capability, and then click the **Mark Row for Delete** icon at the end of the row.
7. When you finish updating the resource, click the **Save Resource** icon.

What to do next

To be able to view the updated resource data in the IBM Intelligent Operations Center user interface, reset the Map. Then, review the resources for an event through the Details portlet.

Creating a resource type

Create a resource type in Tivoli Service Request Manager.

About this task

You can define a hierarchy of resource types, so resource types can have child resource types and so on.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go to > Administration > Classifications**.
3. To view all the existing IBM Intelligent Operations Center resource types, on the **List** tab, in the **Description** field, enter RESOURCE. All the resource types in the hierarchy are displayed.
4. Click the resource type, or child resource type, for which you want to create a child resource type. The classification details for the parent of the new resource type are displayed on the **Classifications** tab.
5. On the **Classifications** tab, under Children, click **New Row**.
6. In the blank row that is appended to the list, enter the following values for the new resource type:
 - a. In the **Classification** column, enter a name.
 - b. In the Classification Desc column, enter a description.
 - c. To prevent the resource type name being changed when you save the resource type, clear the **Generate Description** check box.
7. Click the **Save Classification** icon.
8. To add a graphic icon for the new resource type, do the following substeps:
 - a. Save copies of the graphic in two sizes in PNG format. The larger graphic icon is displayed in the Map portlet, and the smaller graphic icon is displayed in the event list in the Details portlet.

Size 24 pixels x 24 pixels
For example, *new_resource_24.png*

Size 16 pixels x 16 pixels
For example, *new_resource_16.png*
 - b. Copy each PNG file to the appropriate directory on the application server:
 - /opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-24x24/Normal_State
 - /opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-16x16/Normal_State
 - c. Verify that each icon is displayed correctly at the appropriate web browser link:
 - http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png
 - http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png

Adding a capability to a resource type

Create a capability in Tivoli Service Request Manager.

Procedure

1. Log on to the Tivoli Service Request Manager Start Center as an administrator.
2. Click **Go to > Administration > Classifications**.
3. To view all the existing IBM Intelligent Operations Center resource classifications, on the **List** tab, filter for RESOURCE.
4. Click the **Classifications** tab.

5. Under Children, in the list, click the resource type for which you want to add a capability.
6. To prevent the resource name being changed when you save the classification, clear the **Generate Description** check box.
7. Under Attributes, click **New Row**.
8. Enter the details for the new capability:
 - a. For **Attribute**, enter a name.
 - b. In the field on the right of the **Attribute** field, enter a description.
 - c. To enter a value for **Data Type**, click the Select Value icon and choose a value in the Select Value window.
 - d. To specify that child resources inherit this capability, select **Apply Down Hierarchy?**.
9. Click the **Save Classification** icon.

Sample standard operating procedures, workflows, and resources

Sample standard operating procedures, workflows, and resources are provided when you install IBM Intelligent Operations Center Version 1.5.

Standard operating procedures

The following three standard operating procedures are provided:

PLUSIMITIG: Initial preparation for severe weather (Mitigate)

PLUSIMITIG contains the following steps:

1. Validate the severity of the weather. Manual step with no associated workflows.
2. Increase severity rating if needed. Manual step with no associated workflows.

PLUSIPREPA: Prepare for severe weather evacuation (Prepare)

PLUSIPREPA contains the following steps:

1. Prepare evacuation shelters. Manual step with associated workflow PLUSISOP00.
2. Identify evacuation support resources. Manual step with associated workflow PLUSISOP00.
3. Assess support resources availability. Manual step with associated workflow PLUSISOP00.

PLUSIRESPO: Evacuate impacted areas (Respond and Recover)

PLUSIRESPO contains the following steps:

1. Approve evacuation directive. Manual step with no associated workflows.
2. Make sure exit routes are clear. Manual step with no associated workflows.

The standard operating procedure selection matrix is populated with data that triggers the selection of the three standard operating procedures, as shown in the following table:

Table 35. Standard operating procedure selection matrix sample data

| Category | Severity | Urgency | Certainty | Standard operating procedure 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 |

Sample workflow

There is one sample workflow:

PLUSISOP00: Complete the activity action

The PLUSISOP00 workflow triggers an action to change the status of an activity to COMP (complete).

The PLUSISOP00 workflow is associated with each of the steps in the PLUSIPREPA sample standard operating procedure. If you start one of the steps, the status of the step is automatically marked as complete.

Sample resources

The following table lists the sample resources, which are provided in the PLUSICATCPLMAP domain:

Table 36. Sample resources

| Resource | Description | Resource type |
|------------|--------------------------------------|---------------------|
| BASCOMMEYE | Bascombe Eye Institute | RESOURCES\HOSPITAL |
| BLUEFISHW | Blue Fish Warehouse | RESOURCES\WAREHOUSE |
| DOCTORSH | Doctor's Hospital | RESOURCES\HOSPITAL |
| MERYCYH | Mercy Hospital | RESOURCES\HOSPITAL |
| MAMICHILD | Miami Children's Hospital | RESOURCES\HOSPITAL |
| SFFOODDIST | South Florida Food Distribution | RESOURCES\WAREHOUSE |
| TITLEASING | Tropical Trailer Leasing Corporation | RESOURCES\WAREHOUSE |
| UNIMIAMI | University of Miami Hospital | RESOURCES\HOSPITAL |
| WTDCDIST | WTDC Distribution Center Miami | RESOURCES\WAREHOUSE |

Chapter 5. Customizing the solution

Customizing the solution to suit your particular operation includes the tasks covered in this section in relation to the user interface and system properties table. Customizing is closely related to integrating the solution and the appropriate links are included in event and key performance indicator (KPI) topics in this section.

Customizing the user interface

You can customize elements of the IBM Intelligent Operations Center user interface to suit your operation

As well as customizing the layout and appearance of portlets, you can also create new pages. For more information, see the WebSphere Portal product documentation.

Related information:



[IBM WebSphere Portal 7 Product Documentation](#)

Localizing the user interface

Browser settings determine language, date and time settings for the IBM Intelligent Operations Center user interface. An administrator can customize the date and time formats.

In the IBM Intelligent Operations Center, your browser settings determine the language of the text. Where that language is unavailable in the IBM Intelligent Operations Center, the closest relation is used; for example, French Canadian reverts to French which in turn reverts to English which is always available. Your browser settings also determine the time zone for all dates and times that are displayed. Date and time in IBM Intelligent Operations Center are automatically adjusted to the browser's time zone.

All dates and times are presented in your time zone in the format specified in the system properties database table. System properties hold the date and time format strings. To change the value in the database by editing the property, follow the link at the end of the topic.

Related concepts:

“Specifying system-wide configuration data” on page 170

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

“Using CAP for KPI events” on page 92

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

List of portlets

IBM Intelligent Operations Center is a portlet-based solution that uses portal technology to provide tools and display information. All the portlets included in IBM Intelligent Operations Center are listed in the following sections.

User portlets

The following table lists the user portlets included in the IBM Intelligent Operations Center. The table also indicates in which sample page views each portlet is available.

You can customize the portlets. For more information, see the link at the end of the topic.

Table 37. User portlets in the IBM Intelligent Operations Center

| Portlet | Description | Sample page views |
|--|---|---|
| "Contacts" on page 257 | The Contacts portlet can display a list of your contacts that are organized by category. You can organize contacts in categories that are based on the people you need to communicate with. For example, you can have a category for general work contacts and another category for project work contacts. With the Contacts portlet, you can communicate with people and modify your online status, contacts, or groups. | <ul style="list-style-type: none"> • "Supervisor: Status view" on page 253 • "Supervisor: Operations view" on page 254 • "Operator: Operations view" on page 254 |
| "Details" on page 257 | The Details portlet is an interactive list portlet. All the events that you are authorized to see are visible on the events list and on any map portlet linked to the Details portlet. | <ul style="list-style-type: none"> • "Supervisor: Operations view" on page 254 • "Operator: Operations view" on page 254 • "Location Map view" on page 256 |
| "Key Performance Indicator Drill Down" on page 260 | To focus on a specific KPI category in the Key Performance Indicator Drill Down portlet, click the category in the Status portlet. This category is then displayed on its own in the Key Performance Indicator Drill Down portlet. You can use the list to inspect the underlying KPIs until you reach details of the KPI that caused the status change. | <ul style="list-style-type: none"> • "Supervisor: Status view" on page 253 |
| "Location Map" on page 261 | Use the Location Map portlet to see events marked on a location map. A location map in the IBM Intelligent Operations Center is a map or plan with predefined areas for interaction, for example, seating areas in a major sports stadium. | <ul style="list-style-type: none"> • "Location Map view" on page 256 |
| "Map" on page 264 | <p>In the Map portlet:</p> <p>A map of the geographical region with event and resource markers.</p> <p>A filter form to select the categories of the events to be shown on the map and in portlets linked to the Map portlet.</p> <p>A filter form to select the capabilities of the resources to be shown on the map and in the Resources tab on the linked Details portlet. To view this form, first select View Nearby Resources on the Details portlet.</p> | <ul style="list-style-type: none"> • "Supervisor: Operations view" on page 254 • "Operator: Operations view" on page 254 |

Table 37. User portlets in the IBM Intelligent Operations Center (continued)

| Portlet | Description | Sample page views |
|-----------------------------|---|---|
| "My Activities" on page 269 | A user who is logged on can view the activities that are assigned to them in the My Activities portlet. In the My Activities portlet, the activities are grouped by their parent standard operating procedures. Each standard operating procedure corresponds to an individual event. | <ul style="list-style-type: none"> • "Supervisor: Status view" on page 253 • "Supervisor: Operations view" on page 254 • "Operator: Operations view" on page 254 |
| "Notifications" on page 271 | The Notifications portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts. | <ul style="list-style-type: none"> • "Supervisor: Status view" on page 253 • "Supervisor: Operations view" on page 254 • "Operator: Operations view" on page 254 |
| "Reports" on page 272 | Use the Reports portlet to view a report of events as a graph. The portlet provides various options to group events by, and you can choose events by a particular date or date range. These reports help you plan responses to current and future events. | <ul style="list-style-type: none"> • "Supervisor: Reports " on page 255 • "Operator: Reports" on page 255 |
| "Status" on page 274 | The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary. | <ul style="list-style-type: none"> • "Supervisor: Status view" on page 253 |

Related tasks:

"Customizing the portlets" on page 139

As an administrator you can change the portlet settings to customize a portlet.

Administrative portlets

The following table lists the administrative portlets included in the IBM Intelligent Operations Center. The administrative portlets are in the Administration page.

Table 38. Administrative portlets in the IBM Intelligent Operations Center

| Portlet | Description |
|--|---|
| "About" on page 185 | Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation. |
| "Administration Consoles" on page 192 | Use the Administration Consoles portlet to administer the services provided by the solution. |
| "Verifying the components" on page 199 | The System Verification Check tool tests components within IBM Intelligent Operations Center to determine if they are accessible and operational. |

Table 38. Administrative portlets in the IBM Intelligent Operations Center (continued)

| Portlet | Description |
|---|---|
| "User Permissions Summary" on page 76 | The User Permissions Summary portlet displays details of group membership and permissions granted to users. |
| "Key Performance Indicators" on page 160 | In the Key Performance Indicators portlet you can view, change, copy, create, and delete KPIs. You can also customize the KPI hierarchies displayed in the Status and Key Performance Indicator Drill Down portlets. |
| "Location Map Manager" on page 168 | Use the Location Map Manager portlet to customize the Location Map portlet. |
| "Standard Operating Procedures" on page 123 | You can define standard operating procedures and activities to manage events that come into the IBM Intelligent Operations Center. Use the Standard Operating Procedures portlet to access the standard operating procedure, standard operating procedure selection matrix, and workflow designer applications in Tivoli Service Request Manager. |
| "Event Scripting" on page 103 | Use the Event Scripting portlet to write a script to create a sequential list of events to be published at predefined time intervals. |
| "Sample Publisher" on page 99 | The Sample Publisher portlet is an automated test tool intended for an administrator managing or verifying the solution. An administrator can use the Sample Publisher portlet as a client application to test the publication of CAP messages in the IBM Intelligent Operations Center. The Sample Publisher portlet can eliminate the requirement to manually create a test client application. |

Related tasks:

"Customizing the portlets" on page 139

As an administrator you can change the portlet settings to customize a portlet.

Creating or customizing a page

You can create new pages to be included in the IBM Intelligent Operations Center, and specify which portlets to display on those pages. You can customize the appearance and layout of the portlets included on each page.

About this task

Use the WebSphere Portal user interface to customize pages and portlets.

Note: When you create or edit a page layout, ensure that the portlets operate correctly by adhering to the following rules:

- The Map and Details portlets must be in the same group and on the same page to enable adding an event from the Map portlet.
- The My Activities and Details portlets must be in the same group and on the same page to enable requesting event details from the My Activities portlet or requesting Standard Operating Procedure details from the Details portlet.

Procedure

1. To open WebSphere Portal, click the **Administration** tab.
2. In WebSphere Portal, click **Portal User Interface**.
3. Click the required option:

- To work with your pages or create new pages, click **Manage Pages**.
 - To register themes and skins, set the default theme, and set the default skin for each theme, click **Themes and Skins**.
 - To customize the key site elements in themes, including the banner, navigation, fonts, and colors, click **Theme Customizer**.
4. Make the required modifications. For more information about using WebSphere Portal to customize portlets, see the link at the bottom of the topic for the WebSphere Portal product documentation.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Customizing the portlets

As an administrator you can change the portlet settings to customize a portlet.

About this task

There are two possible modes of customization, each changing the portlet settings for all users:

- **Edit Shared Settings** changes the portlet only for the instance of the portlet you are in when you change the settings.
- **Configure** changes the portlet's global settings for all instances of the portlet wherever those instances occur.

The modes of customization that are available to you depend on the permissions associated with your user ID. Global settings are superseded by shared settings.

Procedure

1. Log on to the solution portal as an administrator.
2. Click the upper right corner of the portlet to view the portlet menu.
3. Click **Edit Shared Settings**, or **Configure**.
4. Enter your settings in the fields provided.
5. To close the settings window, click one of the buttons:
 - **Save** to save changes.
 - **Cancel** to cancel changes.
 - **Reset to Defaults** to revert to the default global settings.

Results

Any new settings that you have saved take effect the next time the portlet is refreshed. The default global setting values supplied with the IBM Intelligent Operations Center are used for any parameter which has not been reset.

About portlet settings

Customize the About portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the About portlet. The customization parameters are described in the following table.

Table 39. About portlet customization parameters

| Parameter | Description | Default value |
|-----------|-------------|---------------|
|-----------|-------------|---------------|

Table 39. About portlet customization parameters (continued)

| | | |
|------------------------|---|-----|
| Portlet height | Number of pixels indicating the standard height of the portlet. | 400 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |

Related concepts:

“About” on page 185

Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation.

Administration Consoles portlet settings

Customize the Administration Consoles portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Administration Consoles portlet. The customization parameters are described in the following table.

Table 40. Administration Consoles portlet customization parameters

| Parameter | Description | Default value |
|------------------------|--|--|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | AdministrationConsolePortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 400 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 450 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution is displayed, which is Administration Consoles. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Administration Consoles” on page 192

Use the Administration Consoles portlet to administer the services provided by the solution.

Contacts portlet settings

Customize the Contacts portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Contacts portlet. The customization parameters are described in the following table.

Table 41. Contacts portlet customization parameters

| Parameter | Description | Default value |
|------------------------|--|--|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | SametimeWebClientPortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 250 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Contacts. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Contacts” on page 257

Use the Contacts portlet to send instant messages within the solution.

Details portlet settings

Customize the Details portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Details portlet. The customization parameters are described in the following table.

Table 42. Customization parameters for the Details portlet

| Parameter name | Description | Default value |
|----------------|---|---|
| Columns | Specifications and order of columns to be displayed in the list. | [{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}] |
| Conditions | Additional conditions for the display of events or resources, additional conditions cannot be overridden using the toolbar or map filter. The default is that no additional conditions are applied. | [] |

Table 42. Customization parameters for the Details portlet (continued)

| | | |
|--------------------------------|--|-------------------------|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | CommonEventsPortletHelp |
| Hide add event | True or false setting to hide or display the Add Events button and pop-up menu option. | true |
| Hide add resource | True or false setting to hide or display the Add Resources button on the Resources tab. | true |
| Hide events | True or false setting to hide or display the Events and Incidents tab. | false |
| Hide resources | True or false setting to hide or display the Resources tab. | false |
| Hide toolbar | True or false setting to hide or display the toolbar at the top of the list. | true |
| Ignore cancel resource mode | True or false to acknowledge or ignore incoming resource mode cancellation message from the Map portlet. | false |
| Ignore event creation | True or false setting to acknowledge or to ignore events that are created in the Map portlet by the user. | false |
| Ignore event filter changes | True or false setting to acknowledge or to ignore events filter selections made in the Map portlet by the user. | false |
| Ignore event selection | True or false setting to acknowledge or ignore incoming event selection made in the Map portlet by the user. | false |
| Ignore event tasks | True or false setting to acknowledge or ignore all event pop-up menu selections. | false |
| Ignore map reset | True or false setting to acknowledge or ignore a click of the Resources button on the portlet. | false |
| Ignore resource filter changed | True or false setting to acknowledge or ignore resources filter selections made in the Map portlet by the user. | false |
| Ignore resource tasks | True or false setting to acknowledge or ignore all resource pop-up menu selections. | false |
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between Map, Details, and Location Map portlets on the same page. | default |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 350 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |

Table 42. Customization parameters for the Details portlet (continued)

| | | |
|-----------------|--|---|
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Details. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Note: The explanation of what happens to the portlet title when you provide a resource bundle applies also to the column title which is sourced from the same resource bundle.

Columns parameter

The value of the **columns** parameter is an array of JSON objects which can be configured as explained in Table 43.

Table 43. Objects within the columns parameter value of the Details portlet

| Object | Contains |
|---------------|---|
| id | Column identifier to indicate that the column is to be displayed |
| width | Number of pixels indicating the column width |
| format | String representing the format to be used for date and time columns, the entry overrides the setting in the sysprop table |
| sortAscending | <ul style="list-style-type: none"> Value true to use an ascending sort order on the column items Value false to use a descending sort order on the column items |
| sortPriority | <ul style="list-style-type: none"> Number to indicate the sort priority of that column among all columns, the lower the number, the higher priority No value, leave blank to use the columns default sort priority Value -1 to disable the columns default sort priority |
| title | Column heading title, leave blank to use default heading title |

Columns are displayed in the portlet in the same order as given in the JSON objects that make up the value of the **columns** parameter. Only the columns with the column identifiers specified within the value are displayed, all other columns are hidden. If the value of the **columns** parameter is omitted, the columns are displayed as indicated in the default setting shown in the first row of Table 42 on page 141.

The possible values for the column identifiers are described in Table 44 on page 144.

Table 44. Column identifiers valid for the Details portlet

| Column identifier | Description |
|----------------------------------|---|
| commonevents.id | UUID given to the event in the common events table |
| commonevents.externalEventId | Event identifier assigned by the event submitter |
| commonevents.specification | Format specification followed by the event, for example, CAP |
| commonevents.eventType | Untranslated value for the system-specific code that indicates if an event has been escalated or not: Event or Incident |
| commonevents.sent | Sent time as supplied by the event submitter |
| commonevents.headline | Headline text describing the event |
| commonevents.hover text | Hover text describing the event |
| commonevents.category | Untranslated category value |
| commonevents.certainty | Untranslated certainty value |
| commonevents.severity | Untranslated severity value |
| commonevents.urgency | Untranslated urgency value |
| commonevents.url | URL web address for additional information about the event |
| commonevents.externalWorkOrderId | Associated work order identifier, usually the Tivoli Service Request Manager standard operating procedure ID |
| commonevents.areaId | Location map area identifier if the event is linked to a location map |
| commonevents.largeIcon | Icon used to represent the event on the map |
| commonevents.largeHiliteIcon | Icon used when the event is highlighted on the map |
| commonevents.largeGreyIcon | Icon used when the event is disabled on the map |
| commonevents.smallIcon | Icon used for the event in the list |
| commonevents.user1 | Value set within the Tivoli Netcool/Impact policy |
| commonevents.user2 | Value set by the user within the Tivoli Netcool/Impact policy |
| commonevents.user3 | Value set by the user within the Tivoli Netcool/Impact policy |
| commonevents.user4 | Value set by the user within the Tivoli Netcool/Impact policy |
| commonevents.user5 | Value set by the user within the Tivoli Netcool/Impact policy |

Conditions parameter

The value of the **conditions** parameter is an array of JSON objects which can be configured as described in Table 45.

Table 45. Objects within the conditions parameter value of the Details portlet

| Object type | Contains |
|-------------|--|
| selector | Identifier of the column to which the operator applies |

Table 45. Objects within the conditions parameter value of the Details portlet (continued)

| Object type | Contains |
|-------------|---|
| operator | <p>SQL operator which is applied to the values of the selector; the options are:</p> <ul style="list-style-type: none"> contains when the selector column contains the value, this option is the default equals when the selector column equals the value notEquals the selector column does not equal the value startsWith when the selector column starts with the value endsWith when the selector column ends with the value |
| values | Displayed column value, the value must be the untranslated key value as specified in the previous table |

Note:

The **conditions** parameter defines criteria in addition to those criteria supplied in the filter of the Map portlet. These criteria override the conditions specified in the map filter or in the toolbar.

Note: The toolbar is hidden by default.

For example, you require the following change to columns:

- Display only the **Sent**, **Headline**, **Category**, and **URL** columns.
- Change the **Sent** column width to 12.
- Change the **Sent** column format to d-MMM-yyyy HH:mm.
- Change the sort order priority of the **Sent** column to 2 and **Category** column to 1.

These changes are displayed when you enter the following in the **Columns** field and save your preferences:

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"}, {"id": "commonevents.headline"}, {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

For example, you want to display only events that fulfill both of the following conditions:

- A **Severity** of Extreme or Severe
- An **Event type** of Incident

These changes are displayed when you enter the following in the **Conditions** field and save your preferences:

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]}, {"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

Related concepts:

“Details” on page 257

Use the Details portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

Key Performance Indicator Drill Down portlet settings

Customize the Key Performance Indicator Drill Down portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Key Performance Indicator Drill Down portlet. The customization parameters are described in the following table.

Table 46. Key Performance Indicator Drill Down portlet customization parameters

| Parameter | Description | Default value |
|--------------------------|--|--|
| Columns | Specifications and order of columns to be displayed in the list. | [{"sortPriority": "1", "sortAscending": "true", "id": "kpi.NAME"}] |
| Custom KPI colors | Colors used in the portlet to indicate the status of KPIs, for example, you can enter: {"acceptable": "#7f7f7f", "take_action": "#34333"} The colors you enter here override the colors supplied by the solution. | {} |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | KpiDrillDownPortletHelp |
| Enable KPI filter | True or false setting to enable or disable a KPI filter according to the information in the KPI filter parameter setting. | false |
| Hide toolbar | True or false setting to hide or display the toolbar at the top of the portlet. | true |
| KPI filter | IDs of KPIs to be displayed when the Enable KPI filter is set to true for the portlet, for example, you can enter: ["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"] | [] |
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between Key Performance Indicator Drill Down and Status portlets on the same page. | default |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 350 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Key Performance Indicator Drill Down. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Note: The explanation of what happens to the portlet title when you provide a resource bundle applies also to the column title which is sourced from the same resource bundle.

Columns parameter

The value of the **columns** parameter is an array of JSON objects which can be configured as explained in the following table.

Table 47. Objects within the columns parameter value of the Key Performance Indicator Drill Down portlet

| Object | Contains |
|---------------|--|
| sortPriority | <ul style="list-style-type: none"> • Number to indicate the sort priority of that column among all columns, the lower the number the higher priority • No value, leave blank to use the column's default sort priority • -1 to disable the column's default sort priority |
| sortAscending | <ul style="list-style-type: none"> • true to use an ascending sort order on the column items • false to use a descending sort order on the column items |
| id | Column identifier to indicate that the column is to be displayed |

Columns are displayed in the portlet in the same order as given in the JSON objects that make up the value of the **columns** parameter. Only the columns with the column identifiers specified within the value are displayed, all other columns are hidden. If the value of the **columns** parameter is omitted, the columns are displayed as indicated in the default setting shown in the first row of Table 46 on page 146.

The possible values for the column identifiers are described in the following table.

Table 48. Column identifiers valid for the Key Performance Indicator Drill Down portlet

| Column identifier | Description |
|----------------------|-----------------------------|
| kpi.NAME | Name of the KPI |
| kpi.CURRENT.VALUE | Current value of the KPI |
| kpi.CURRENT.STATUS | Current status of the KPI |
| kpi.CALCULATION.TIME | Time the KPI was calculated |

Related concepts:

“Key Performance Indicator Drill Down” on page 260

Use the Key Performance Indicator Drill Down portlet to see more information about a KPI category, the status of its underlying KPIs.

Key Performance Indicators portlet settings

Customize the Key Performance Indicators portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Key Performance Indicators portlet. The customization parameters are described in the following table.

Table 49. Key Performance Indicators portlet customization parameters

| Parameter | Description | Default value |
|------------------------|--|--|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | KpiManagerPortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 500 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Key Performance Indicators. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

Location Map portlet settings

Customize the Location Map portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the portlet. The customization parameters are described in the following table.

Table 50. Location Map portlet customization parameter values

| Parameter | Description | Default value |
|------------------------------|---|--|
| Default filter selections | Default event categories to be displayed on the map. Enter the name or names separated by a semicolon and without spaces. | CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other |
| Default area highlight color | Default color of an area that is highlighted when you hover over the area using your cursor. | #808080 |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | LocationMapPortletHelp |
| Default map selection | Name of the location map to be displayed in the portlet. | Miami SunLife Stadium |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 400 |

| | | |
|--------------------------|--|--|
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between Map, Details, and Location Map portlets on the same page. | default |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Location Map. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Location Map” on page 261

Use the Location Map portlet to see events marked on a location map. A location map in the IBM Intelligent Operations Center is a map or plan with predefined areas for interaction, for example, seating areas in a major sports stadium.

Location Map Manager portlet settings

Customize the Location Map Manager portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the portlet. The customization parameters are described in the following table.

Table 51. Location Map Manager portlet customization parameter values

| Parameter | Description | Default value |
|---------------------------------------|--|-------------------------------|
| Default color for selected new area | Default color of an area that is drawn on the map and selected. | #4AA02C |
| Default color for selected saved area | Default color of an area on the map that is saved and selected. | #808080 |
| Default color for new area | Default color of an area that is drawn on the map. | #009900 |
| Default color for saved area | Default color of an area that is saved on the map. | #808080 |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | LocationMapManagerPortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 400 |

| | | |
|-----------------|--|--|
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Location Map Manager. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Location Map Manager” on page 168

Use the Location Map Manager portlet to customize the Location Map portlet.

Map portlet settings

Customize the Map portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Map portlet. The customization parameters are described in the following table.

Table 52. Customization parameter values

| Parameter | Description | Default value |
|------------------|---|---------------|
| Center latitude | Specific coordinates to set the center point of the map. The current location of the map is displayed to the right of the fields. You can zoom and pan the map to your required location, then cut and paste the values shown into the corresponding fields. | 25.780416 |
| Center longitude | | -80.203629 |
| Zoom level | Standard magnification level for the map. The range of valid zoom levels available is dependent on the base map. Generally, the range is from 1 upwards. The value of 1 is the lowest zoom level which displays the map at its lowest magnification. For example, the default ArcGIS base map supplied with the solution displays geographical detail up to a maximum of zoom level 12. | 11 |
| Base layer type | Value for the type of the base map. | ARC_GIS_REST |

Table 52. Customization parameter values (continued)

| | | |
|--------------------------------|---|---|
| Base layer URL | URL of the base map. The URL must contain, in the correct order, the placeholders that represent the x, y, and z coordinates of the map. You can select a map from your installed Esri GIS server or a publicly available GIS service. | http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x} |
| KML feed or file URL | URL to display KML data. Enter a URL for a location on the same server as the portlet with the same domain and port. To ensure that you implement this condition, enter only URLs that start with '/' or forward slash character, so that the browser selects the current domain and port. For multiple URL strings use a semicolon and no spaces between URLs. If the required web site is not local, use a proxy server on your portal server to access the site. Note: Use this option for small local adjustments, but consider the amount of data involved, so that it is not overwhelming the display or affecting performance. | There is no default value supplied with the solution. |
| The amount of items to display | Limit for the number of markers displayed on a view. Enter the maximum number of markers that can be displayed. If the number of markers in the area of the map in view exceeds this limit, no markers are shown and a warning message is displayed. The user can then choose whether to load the markers or change the view. | 250 |
| Default filter selections | Default event categories to be displayed on the map. Enter the name or names separated by a semicolon and without spaces. | CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between Map, Details, and Location Map portlets on the same page. | default |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Map. |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | NavigatorPortletHelp |

Table 52. Customization parameter values (continued)

| | | |
|-----------------|--|--------------------------------------|
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |
|-----------------|--|--------------------------------------|

Related concepts:

“Map” on page 264

Use the Map portlet to see events and resources on a map.

My Activities portlet settings

Customize the My Activities portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the My Activities portlet. The customization parameters are described in the following table.

Table 53. My Activities portlet customization parameters

| Parameter | Description | Default value |
|--------------------------|--|---|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | ActivitiesPortletHelp |
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between portlets on the same page. For example, a common name can set up communication between My Activities and Details portlets. | default |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 200 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: My Activities. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“My Activities” on page 269

The My Activities portlet displays a dynamic list of activities that are owned by the group of which the user, who is logged on to the interface, is a member.

Notifications portlet settings

Customize the Notifications portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Notifications portlet. The customization parameters are described in the following table.

Table 54. Notifications portlet customization parameters

| Parameter | Description | Default value |
|------------------------|--|---|
| Columns | Specifications and order of columns to be displayed in the list. | [{"id": "notifications.HEADLINE"}, {"id": "notifications.SENTFROM"}, {"id": "notifications.SENTTIME", "width" : "10", "format": "yyyy-MM-dd HH:mm:ss"}] |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | CityCoordinatorPortletHelp |
| Hide toolbar | True or false setting to hide or display the toolbar at the top of the portlet. | true |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 200 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Notifications. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Note: The explanation of what happens to the portlet title when you provide a resource bundle applies also to the column title which is sourced from the same resource bundle.

Columns parameter

The value of the **columns** parameter is an array of JSON objects which can be configured as explained in Table 55.

Table 55. Objects within the columns parameter value of the Notifications portlet

| Object | Contains |
|--------|--|
| id | Column identifier to indicate that the column is to be displayed |
| width | Number of pixels indicating the column width |

Table 55. Objects within the columns parameter value of the Notifications portlet (continued)

| Object | Contains |
|---------------|---|
| format | String representing the format to be used for date and time columns, the entry overrides the setting in the sysprop table |
| sortAscending | <ul style="list-style-type: none"> • true to use an ascending sort order on the column items • false to use a descending sort order on the column items |
| sortPriority | <ul style="list-style-type: none"> • Number to indicate the sort priority of that column among all columns, the lower the number, the higher priority • No value, leave blank to use the columns default sort priority • -1 to disable the columns default sort priority |
| title | Column heading title, leave blank to use default heading title |

Columns are displayed in the portlet in the same order as given in the JSON objects that make up the value of the **columns** parameter. Only the columns with the column identifiers specified within the value are displayed, all other columns are hidden. If the value of the **columns** parameter is omitted, the columns are displayed as indicated in the default setting shown in the first row of Table 54 on page 153.

The possible values for the column identifiers are described in Table 56.

Table 56. Column identifiers valid for the Notifications portlet

| Column identifier | Description |
|---------------------------|--|
| notifications.ID | UUID given to the notification in the notification table |
| notifications.CATEGORY | Untranslated value of the category of the event or KPI related to the notification |
| notifications.SENTFROM | Service that generated the notification |
| notifications.SENTTOGROUP | List of groups that can access the notification |
| notifications.SENTTIME | Time generated by the service that submitted the notification |
| notifications.HEADLINE | Short text describing the notification |
| notifications.DESCRPTION | Detailed text describing the notification |
| notifications.ALERTLINK | List of CAP alerts related to the notification |
| notifications.KPILINK | KPI related to the notification |

Related concepts:

“Notifications” on page 271

Use the Notifications portlet to view your alert messages and their details.

Reports portlet settings

Customize the Reports portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the portlet. The customization parameters are described in the following table.

Table 57. Reports portlet customization parameter values

| Parameter | Description | Default Value |
|------------------------|---|---|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | ReportsIntegrationPortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 600 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 800 |
| Portlet title | Title of the Reports portlet. | Custom Report |
| Report URL | Specifies the URL of the report that is displayed. | http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as shown in the Portlet title field of the Shared Settings window. | There is no default resource bundle. |
| Show URL field on page | Select True to include the Report URL button on the Reports portlet page. This button enables all users, not just administrators, to create a custom report and set the report URL. Select False to omit the Report URL button from the Reports portlet page. | False |

Related concepts:

“Reports” on page 272

Use the Reports portlet to view a report of events as a graph. The portlet provides various options to group events by, and you can choose events by a particular date or date range. These reports help you plan responses to current and future events.

Sample Publisher portlet settings

Customize the Sample Publisher portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Sample Publisher portlet. The customization parameters are described in the following table.

Table 58. Sample Publisher portlet customization parameters

| Parameter | Description | Default value |
|------------------|--|--|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | SamplePublisherPortletHelp |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Sample Publisher. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |

Related concepts:

“Sample Publisher” on page 99

Use the Sample Publisher portlet to publish Common Alerting Protocol (CAP) events into the IBM Intelligent Operations Center.

Standard Operating Procedures portlet settings

Customize the Standard Operating Procedures portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Standard Operating Procedures portlet. The customization parameters are described in the following table.

Table 59. Standard Operating Procedures portlet customization parameters

| Parameter | Description | Default value |
|------------------|--|-----------------------|
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | SOPManagerPortletHelp |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 440 |

Related concepts:

“Standard Operating Procedures” on page 123

You can define standard operating procedures and activities to manage events that come into the IBM Intelligent Operations Center. Use the Standard Operating Procedures portlet to access the standard operating procedure, standard operating procedure selection matrix, and workflow designer applications in Tivoli Service Request Manager.

Status portlet settings

Customize the Status portlet by changing the settings in the fields of the **Shared Settings** window.

Customization parameters

The fields of the **Shared Settings** window contain the values of the customization parameters for the Status portlet. The customization parameters are described in the following table.

Table 60. Status portlet customization parameters

| Parameter | Description | Default value |
|--------------------------|--|--|
| Custom KPI colors | Colors to be used in the portlet to indicate the status of KPIs, for example, you can enter: <pre>{"acceptable": "#7f7f7f", "take_action": "#343333"}</pre> The colors you enter here override the colors supplied by the solution. | {} |
| Default help JSP | Name of the JSP help file to be shown when the help is selected from the portlet menu. | KpiStatusPortletHelp |
| Enable KPI filter | True or false setting to enable or disable an additional KPI filter for the portlet according to the information in the KPI filter parameter value. | false |
| KPI filter | IDs of KPIs to be displayed when the 'Enable KPI filter' is set to true for the portlet, for example: <pre>["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]</pre> | [] |
| Portlet group identifier | Name of the group to which this portlet belongs. A common name sets up communication between Key Performance Indicator Drill Down and Status portlets on the same page. | default |
| Portlet height | Number of pixels indicating the standard height of the portlet. | 200 |
| Portlet maximum height | Number of pixels indicating the maximum height for the portlet. | 600 |
| Portlet title | Title to override the title supplied with the solution. | If you do not enter a value for this parameter, the title supplied by the solution and displayed is: Status. |
| Resource bundle | Location of the resource bundle you provide as a source for the value of properties, for example, portlet title. This location is required if you want to specify the title as a property key in a resource bundle you provide. If no resource bundle is specified, then the key is not looked for and the title is displayed as supplied by the solution. | There is no default resource bundle. |
| Show legend | True or false setting to hide or display the legend in the portlet. | true |
| Sort order | KPI property by which the KPI list is sorted. The default is to sort in ascending alphabetic order by KPI name. Other options are <code>kpi.CURRENT.VALUE</code> , <code>kpi.CURRENT.STATUS</code> , and <code>kpi.CALCULATION.TIME</code> | +kpi.NAME |

Related concepts:

“Status” on page 274

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

Customizing the portlet help

You can deploy alternative help for an IBM Intelligent Operations Center portlet.

About this task

For help using each portlet, click the upper right corner of the portlet, and select **Help** from the menu displayed.

If you change the layout or the data displayed in a portlet, you might also want to change the help displayed.

Procedure

1. Create the alternative help as a JSP file.
2. You can give the file any name you want, but you must use the correct suffix for your language. The language setting is based upon the language of our browser. Use the standard locale identifier for your language, for example:

| Option | Description |
|---------------------|----------------------|
| <code>_pt_BR</code> | Brazilian Portuguese |
| <code>_en</code> | English |
| <code>_fr</code> | French |
| <code>_de</code> | German |
| <code>_es</code> | Spanish |

3. Use the portlet **Shared Settings** window to set the **DefaultHelpJSP** parameter with the alternative help file name. Do not include the language suffix or .jsp file extension.
4. Copy the alternative help JSP file to the correct location: `/opt/IBM/WebSphere/wp_profile/installedApps/cell1/ioc_portal_ear.ear/portlet_war/portlet_root/jsp/html/help`. The values for each portlet of the `portlet_war` and `portlet_root` variables are listed in a separate topic. See the link at the end of this topic for a list of these values.

Note: When changing the User Permissions Summary help file, replace `ioc_portal_ear.ear` with `iss_portal_ear.ear` in the path given in this step.

What to do next

Provide translations of the alternative help file for all supported languages including a default language.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Portlet help file locations

Location values are required for each portlet when replacing the default portlet help with your alternative JSP help file.

Table 1 and 2 give values for the location of user and administration portlet help files.

Table 61. User portlet values for location of an alternative help file

| Portlet | portlet_war | portlet_root |
|--------------------------------------|--------------------------------------|-----------------------------------|
| Details | icoc_ui_common_events_portlet.war | _icoc_ui_common_events_portlet |
| Key Performance Indicator Drill Down | icoc_ui_kpi_drilldown_portlet.war | _icoc_ui_kpi_drilldown_portlet |
| Location Map | icoc_ui_location_map_portlet.war | _icoc_ui_location_map_portlet |
| Map | icoc_ui_navigator_portlet.war | _icoc_ui_navigator_portlet |
| My Activities | icoc_ui_activities_portlet.war | _icoc_ui_activities_portlet |
| Notifications | icoc_ui_city_coordinator_portlet.war | _icoc_ui_city_coordinator_portlet |
| Reports | icoc_ui_reports_portlet.war | _icoc_ui_reports_portlet |
| Status | icoc_ui_kpi_status_portlet.war | _icoc_ui_kpi_status_portlet |

Table 62. Administration portlet values for location of an alternative help file

| Portlet | portlet_war | portlet_root |
|-------------------------------|--|---|
| Administration Consoles | icoc_ui_administration_console_portlet.war | _icoc_ui_administration_console_portlet |
| Event Scripting | icoc_ui_event_scripting_portlet.war | _icoc_ui_event_scripting_portlet |
| Key Performance Indicators | icoc_ui_kpi_manager_portlet.war | _icoc_ui_kpi_manager_portlet |
| Location Map Manager | icoc_ui_location_map_manager_portlet.war | _icoc_ui_location_map_manager_portlet |
| Sample Publisher | icoc_ui_sample_publisher_portlet.war | _icoc_ui_sample_publisher_portlet |
| Standard Operating Procedures | icoc_ui_sop_manager_portlet.war | _icoc_ui_sop_manager_portlet |
| User Permissions Summary | iss_ui_security_portlet.war | _iss_ui_security_portlet |

Customizing KPIs

In the IBM Intelligent Operations Center you can customize Key Performance Indicator (KPI) models to suit your business processes.

KPIs are designed to supply statistical data that can be used to analyze trends or to indicate problem areas. KPI data is updated by events within the IBM Intelligent Operations Center.

The IBM Intelligent Operations Center provides a set of sample KPIs and events that can be used to update KPI status. There are three sample KPI models supplied with the IBM Intelligent Operations Center based on sample public safety, transportation and water monitoring and business processes. For more information about the sample KPIs provided with the IBM Intelligent Operations Center, follow the link at the end of the topic.

Each IBM Intelligent Operations Center solution follows a KPI creation and integration process to set up the KPIs required for the specific business environment. You can create your own KPI models with the IBM WebSphere Business Monitor. For more information about creating and integrating KPIs with the IBM Intelligent Operations Center, follow the link at the end of the topic.

Use the Key Performance Indicators portlet to customize KPIs in the IBM Intelligent Operations Center. The Key Performance Indicators portlet is provided for the administrator as one of the **Solution Customization Tools** options.

Using the portlet, you can view KPI properties; create, copy, or modify KPIs; and view or change the hierarchical displays for KPI models.

Use the **KPI Definition** tab to define the KPIs associated with a specific KPI model in the IBM Intelligent Operations Center:

- View the current list of KPIs belonging to a KPI model.
- View the properties of an existing KPI.
- Update the properties of an existing KPI.
- Create a new KPI for a KPI model:
 - Aggregate KPI calculated using a defined metric
 - Expression KPI value based on other KPIs
- Delete a KPI.

Your updates are saved to IBM WebSphere Business Monitor models stored in the IBM Intelligent Operations Center database. Your updates are also reflected at the next refresh of the Status and Key Performance Indicator Drill Down portlets.

Use the **KPI Display Hierarchy** tab to update the KPI hierarchies displayed in the Status and Key Performance Indicator Drill Down portlets.

- View the existing KPI hierarchies.
- View the main properties of a KPI.
- Change the tree structure by moving or removing items in a KPI hierarchy.
- Add pre-defined KPIs to a hierarchy.

Your updates are reflected at the next refresh of the Status and Key Performance Indicator Drill Down portlets.

Note: Any updates to the display hierarchy are independent of the KPI model and an understanding of the KPI model is necessary to ensure that updates adhere to the logic of the KPI model.

Related concepts:

“Creating and integrating KPIs” on page 105

Key performance indicator (KPI) models can be created and modified using a business monitoring development toolkit and a KPI management portlet.

“Sample KPIs” on page 117

Sample KPIs are provided with the IBM Intelligent Operations Center. The sample KPIs are designed to provide guidance for implementing different types of KPI using the IBM WebSphere Business Monitor Development Toolkit. Sample monitor models are provided for water, transportation and public safety.

Key Performance Indicators

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

In the Key Performance Indicators portlet you can view, change, copy, create, and delete KPIs. You can also customize the KPI hierarchies displayed in the Status and Key Performance Indicator Drill Down portlets.

To access the Key Performance Indicators portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Key Performance Indicators**.

Viewing KPI hierarchies

Use the **Relationships and Display** tab to view KPI models as they are displayed in the Status and Key Performance Indicator Drill Down portlets.

About this task

On the left of the **Relationships and Display** window, you see listed the root level nodes for the KPI hierarchies that you are authorized to view. These nodes represent the KPI models as they are displayed on the Status and Key Performance Indicator Drill Down portlets.

Procedure

1. Expand a root level node to see lower levels of the model tree you want to view.
2. Click a root level node title to preview its details on the right of the window. The information is displayed as described in the following table:

| Option | Description |
|----------|--|
| Name | title of the root level node |
| Type | type of root level node |
| Model ID | identifier for the corresponding KPI model |
| Category | classification of the model |
| Icon | icon that represents the root level node |

3. Click a KPI to preview its details on the right of the **Relationships and Display** window.

Changing a KPI hierarchy

Use the **Relationships and Display** tab to change or remove a KPI model as it is displayed in the Status and Key Performance Indicator Drill Down portlets.

Procedure

1. On the left of the **Relationships and Display** window, click the root level node and subitems to expand the hierarchical tree to the level that you want.
2. You can move, add, change, or remove existing items, as follows:
 - To move subitems within a tree, drag the item to the position you require. Green or red indicators indicate whether a move is allowed or not.
 - To add to a tree from the list of existing subitems for a KPI model, right-click on the item to contain the subitem and click **Add KPI**.
 - To go to the **KPI Properties** window and change a subitem, right-click on the item and click **Edit**.
 - To remove a root level node or a subitem from a tree, right-click the item and click **Remove**. Removing a root node item removes all of the subitems it contains.
3. Click **Save** to save your updates.

Note: It is not possible here to edit the name of an owning organization or root level node. If you want to change an owning organization, remove it and replace it with another name.

Adding an owning organization

Use the **Relationships and Display** tab to add a root level node to be displayed on the Status and Key Performance Indicator Drill Down portlets.

Procedure

1. At the upper left of the **Relationships and Display** window, click **Add Owing Organization**
2. Type in a display name.
3. From the drop-down list of the **Model** field, select the root level node to be added.
4. From the drop-down list of the **Category** field, select a category for the root level node.
5. From the drop-down list of the **Icon** field, select the file name for the icon to represent the root level node.

6. Click **OK** to add the new node on the left of the **Relationships and Display** window.
7. Click **Save** to update the display in the Status and Key Performance Indicator Drill Down portlets.

Changing the KPI legend

Use the **Relationships and Display** tab to change the KPI legend on the Status portlet.

Procedure

1. At the upper left of the **Relationships and Display** window, click **KPI Legend**.
2. Change the display for the KPI legend as follows:
 - To add a range, click **Add Row**.
 - To change a range, edit the fields under **Range Name, Color, Icon**.
 - To delete a range, click **Delete**.
3. Click **OK** to update the display on the Status and Key Performance Indicator Drill Down portlets.

Viewing a KPI model

Use the **KPI Definition** tab to view KPIs belonging to the KPI models within the IBM Intelligent Operations Center.

Procedure

The **Filter by model** field contains a drop-down list of business process models that you are authorized to view. Select all models or the model for which you want to see KPIs. The KPI information is displayed as described in the following table:

| Option | Description |
|-----------------|---|
| KPI Name | Title of the KPI. You can click the KPI name to see the properties. |
| Model | Name of the model the KPI belongs to. |
| Created | Method of creation of the KPI: <ul style="list-style-type: none"> • A modeled KPI is a KPI created at the model level using IBM WebSphere Business Monitor. • A Dashboard KPI is a KPI created using the Key Performance Indicators portlet. |
| Type | Type of KPI: <ul style="list-style-type: none"> • An aggregate KPI has a value that is based on the metric and aggregation method you select. • An expression KPI has a value that is based on other KPIs or user-defined functions, using an XPath expression that you define. |
| Access | Access level of a KPI: <ul style="list-style-type: none"> • A shared KPI is a KPI that other users have access to view. • A private KPI is a KPI that cannot be shared with users other than the owner. |

Viewing or changing a KPI

Use the **KPI Definition** tab to view or change an existing KPI belonging to a model in the IBM Intelligent Operations Center.

Procedure

1. Select a KPI. At the upper left of the **KPI Definition** window, click **Edit**. The **KPI Properties** window opens.

2. To change the KPI, edit the fields on the tabs of the properties window. For more details about editing these fields to create an aggregate or expression KPI, click the link at the end of the topic.

Note: You cannot change the definition of a modeled KPI here.

3. To save and exit from the updated **KPI properties** window, click **OK**. To save and continue changing the copied KPI, click **Apply**. To exit without saving, click **Cancel**.

Copying a KPI

Use the **KPI Definition** tab to make a copy of an existing KPI for a model in the IBM Intelligent Operations Center.

Procedure

1. Select a KPI. At the upper left of the **KPI Definition** window, click **More Actions > Copy**. The **KPI properties** window opens.
2. Type a new KPI name in the **KPI Name** field.
3. Edit the properties of the copied KPI according to steps 3 and 4 of the procedure for changing a KPI.

Creating a KPI

Use the **KPI Definition** tab to create a KPI for a model in the IBM Intelligent Operations Center.

Procedure

1. At the upper left of the **KPI Definition** window, click **Create**.
2. Click **New Aggregate KPI** or **New Expression KPI**. The **KPI Properties** window opens.
3. Edit the properties of the new KPI according to steps 3 and 4 of the procedure for changing a KPI.

What to do next

For more information about creating KPIs, go to IBM Websphere Business Monitor documentation link at the end of the topic.

Sample KPIs

A set of sample KPIs is provided with the solution. These KPIs are designed to provide guidance for planning and implementing different types of KPIs to suit your organization. Examples are provided in the areas of water, transportation, and public safety.

Customizing the Key Performance Indicators portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related concepts:

“Status” on page 274

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

“Key Performance Indicator Drill Down” on page 260

Use the Key Performance Indicator Drill Down portlet to see more information about a KPI category, the status of its underlying KPIs.

Related reference:

“Key Performance Indicators portlet settings” on page 147

Customize the Key Performance Indicators portlet by changing the settings in the fields of the **Shared Settings** window.

Related information:

 IBM WebSphere Business Process Management Version 7.0 Information Center

Back up before customizing KPIs

Back up and restore KPIs which have been created or modified with IBM WebSphere Business Monitor, or with the Key Performance Indicators portlet.

About this task

Before you customize KPI models and modify KPIs, you might want to back up existing models. The procedure in this topic exports all KPIs from the specified model to the specified file, and imports KPIs from the specified file to the specified model.

Procedure

1. Log on to the application server.
2. Change to the bin directory of the IBM WebSphere Business Monitor profile: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin`
3. To export KPIs, run the command: `./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/exportKpis.jy" "xml_file_path" model_ID model_version ALL`
xml_file_path is the name and path of the XML file to which you are exporting KPIs. *model_ID* and *model_version* are the ID and version of the KPI model from which you are exporting KPIs.
4. To import KPIs, run the command: `./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/importKpis.jy" "xml_file_path"`
xml_file_path is the name and path of the XML file from which you are importing KPIs.

Example

To export all KPIs from the model, `icoc_sample_public_safety_monitor_model`, to `/tmp/kpis.xml`, run the following command. In the command, the value of *xml_file_path* is `/tmp/kpis.xml`, the value of *model_ID* is `icoc_sample_public_safety_monitor_model`, and the value of *model_version* is `2011-02-18T10:49:46`.

```
./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model 2011-02-18T10:49:46 ALL
```

For more information, see the link to the WebSphere Business Monitor information center at the end of the topic.

Related reference:

“Backing up data” on page 245

To prevent the loss of valuable data in IBM Intelligent Operations Center, back up certain files, directories, and databases at regular intervals.

Related information:

 IBM Smarter Cities Software Solutions Redbooks

Customizing event correlation

This section explains event correlation, and describes how to change and create new decision tables. It also explains the rules application.

Event correlation and the rules application

This topic provides an overview of the event correlation process and briefly explains the rules application.

The event correlation rules application based in WebSphere Operational Decision Management enables you to modify and extend correlation rules without advanced technical knowledge of IBM Intelligent Operations Center or WebSphere Operational Decision Management. However, basic knowledge of Common Alerting Protocol events and of WebSphere Operational Decision Management is required.

Three variables determine how events correlate: the source event, the target event, and the decision table.

For each incoming Common Alerting Protocol event, the rules application is called to determine if any of the existing events correlate with the incoming event. The source event is always the new incoming event and it triggers the correlation. The correlation process checks the source event against events in the database. When an event is found in the database that correlates with the source event, this event is called the target event. Anytime a possible correlation is found, the Notifications portlet sends an alert.

The determination is unidirectional. This concept is important because the rules that determine the correlation do not have to be symmetrical. For example, if event A correlates to event B, it does not mean that event B correlates to event A.

The rules application provides one sample correlation table that suits most requirements. Refer to “Customizing event correlation settings” for different ways of customizing the correlation rules.

Customizing event correlation settings

This section explains how to customize event correlation settings.

The decision table, which can be edited in the Decision Center, has two types of columns. Columns on the left are called decision columns. They determine which action column, on the right, to use. The decision tables are checked from left to right and, depending on the values of the different rows, lead to an action column on the right. The action column defines what is run when a specific row is reached.

The recommended way to expand and modify event correlation settings is to edit an existing decision table. The following items describe how decision tables are formatted:

- On the left side of the decision table (white background) are the decision columns. They determine which of the rows in the action columns (grey background) are executed.
- The last action column in the table calls the query and publication service. If there is an action row that you do not want as a correlation query and publication, deactivate the entry in this last column.
- The set SQL Query column in the action columns can override the query parameters. Overriding query parameters is cumbersome and unneeded for most applications. The requirement for this query is that there be three named columns in the query result:

- event_headline - The title to be used in the description of the correlation. This text becomes the notification description.
- event_external_id - The external id, such as CAP-ID, of the event
- event_internal_id - The internal id, such as CapAlertId, to be used by the Notifications portlet to map to headlines in the **Refers to Alerts** field of the notification properties.

This section contains the following topics:

Modifying decision properties

Use the Decision Center user interface in WebSphere Operational Decision Management to change event correlation settings. This topic explains more information about changing decision properties in the decision tables. It also provides a link to the WebSphere Operational Decision Management documentation.

About this task

The user interface is located on node 1 of the installation of the portal server at this URL: http://app_server:9084/teamserver. Log on as waswebadmin.

Most of the changes you make can be done within the rules application as described in “Editing the decision table.” Other modifications might involve changes to the following:

- The Tivoli Netcool/Impact policies
- The WebSphere Message Broker Java compute node that transforms the messages from the impact policies to the message driven bean format
- The query Executable Object Model (XOM) and the Business Object Model (BOM)

For more information and instructions for modifying the XOM and BOM, information for the message broker node, and information about the Decision Center refer to the WebSphere Operational Decision Management and WebSphere Message Broker information centers using the links below.

Related information:

 [IBM WebSphere Operational Decision Management Information Center](#)

 [WebSphere Message Broker documentation](#)

Editing the decision table

This topic provides a brief explanation of the decision table, and provides steps for changing the decision table properties.

In the IBM Intelligent Operations Center WebSphere Operational Decision Management rules application, there is a basic correlation table defined that uses the category and type of the event to determine which action row to execute.

Currently, the action rows are identical, but can be changed to fit your requirements. For example, you can define that fire events are treated differently from other events and only correlate with water and other fire events. To change values to fit your requirements, activate the Categories column cell for the row and enter "Fire, Water" in the cell. If you want the rule to distinguish between Events and Incidents, add a row to this decision column and the action column accordingly.

To change the radius of the search for correlated events, change the **Set search radius** value. The entered integer is interpreted as meters from the center of the source event. So, if you enter 2000, it correlates only with events that are fewer than 2000 meters away from the source event.

Changing decision table properties Procedure

1. Log on to `http://app_server:9084/teamserver` as `rtsadmin`.
2. Go to your browser's explorer.
3. Click **capCorrelationRules**.
4. Click **simpleCorrelationPolicy**.
5. Click **Edit**. The properties page is displayed.
6. Click **Next** on the properties page.
7. Edit the table. For examples of columns that you can add to the decision table, see the template provided in the templates folder.
8. When you finish making properties changes to the table, click **Finish**.

What to do next

Export the rules application from the Decision Center using the related link below.

Related tasks:

“Deploying the modified rule set to the IBM Intelligent Operations Center flow”
Use this topic to deploy the modified rule set to the rule execution server.

Deploying the modified rule set to the IBM Intelligent Operations Center flow

Use this topic to deploy the modified rule set to the rule execution server.

About this task

When you modify any properties or items in the decision table, you must deploy the modified rule set to the event flow in the IBM Intelligent Operations Center. After deploying the modified rule set to the rule execution server, the correlation rules work differently depending on your changes. The rule execution server checks the incoming events for possible correlations.

To deploy the modified rule set, complete the following steps.

Procedure

1. Export the rules application from the Decision Center:
 - a. Go to `app_server:9084/teamserver/`.
 - b. Log on as `rtsadmin`.
 - c. Navigate to **Project > Generate RuleSet**.
 - d. Click **Next**, select nothing, and download the RuleApp jar file.
2. Import the rules application into the rule execution server:
 - a. Go to `app_server:9083/res`.
 - b. Click the Explorer tab.
 - c. Click **icoc_wodm_correlation_ruleApp > Add Ruleset**.
 - d. Name the rule set and note the path of the new rule set: `/icoc_wodm_correlation_ruleApp/1.0/
yourChosenName/version`.
Where
 - *yourChosenName* is the name you choose for the rules set
 - *version* is the version of the rules set
3. Set the new path of the rules set in the impact policy:
 - a. Go to `event_server:9080/nci/login_main.jsp`.
 - b. From the drop-down menu on the left, select IBM Intelligent Operations Center.

- c. Click **Policies**, and select the **IOC_Event_Correlation** policy.
- d. Change the value of the field: **JMSProps.ilog_rules_bres_mdb_rulesetPath** to the new path:
`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`.
Where
 - *yourChosenName* is the name you chose for the rules set
 - *version* is the version of the rules set
- e. Click **Save**.

Related tasks:

“Changing decision table properties” on page 167

Location Map Manager

Use the Location Map Manager portlet to customize the Location Map portlet.

You can customize the following aspects of the Location Map portlet:

- Classification name to be displayed on the menu on the left of the portlet.
- Map to be displayed in the portlet.
- Areas within a map.

Areas within a map are identified by an area identifier code. Any event with an area identifier code appears on all location maps with that area defined.

There is also an option to give an area a parent identifier. You can use the parent identifier to create an area hierarchy. For example, create areas to represent the seating stands on the first floor of a sports stadium. Each seating stand is defined on the detailed location map of the first floor of the stadium. Additionally, give each seating stand a parent identifier to indicate that it is on the first floor of the stadium. An event with an area identifier for one of the seating stands appears on the detailed seating map of the first floor. This event also appears on an overview map of the stadium because the first floor here has the same area identifier used as a parent identifier for the seating stands.

To access the Location Map Manager portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Location Map Manager**.

Adding a classification to the map menu

Use the **Classifications** tab to add a classification to display in map menu of the Location Map portlet.

Procedure

1. Enter a name in the **Classification Name** field. You have the option to add a description.
2. To add your classification to the portlet, click **Submit**.

Results

Your new classification appears on the Location Map portlet when you refresh the portlet page.

Adding a map to the portlet

Use the **Location Maps** tab to add a location map to display in the Location Map portlet.

Procedure

1. Enter a name in the **Classification Name** field. You can select from the drop-down list.
2. Enter a location map name in the **Map Name** field. You have the option to add a description of the map.

3. Enter a URL for the location map in the **Image** field.
4. To add your map to the menu, click **Submit**.

Results

Your map appears on the Location Map portlet menu when you refresh the portlet page. You can then select and view the map.

Adding or changing areas on a location map

Use the **Areas** tab to create new areas, change areas, or remove areas for display on a location map in the Location Map portlet.

Procedure

1. Enter a map name in the **Map Name** field. You can select from the drop-down list of maps.
2. To draw a new area on the map, click the polygon symbol in the upper right corner of the box. Click the required position on the map and then click each corner to draw a polygon. Double-click to finish the polygon. New areas appear in green by default.
3. To enter details for an area, click the hand symbol in the upper right corner of the box. Click the area to be updated.
4. Enter an area map name in the **Area Name** field. You have the option to add a description.
5. Enter an area identifier in the **Area Identifier** field. You have the option to add a parent area identifier.
6. To update an area on the map, click **Update Area**. To remove an area on the map, click **Remove Area**.
7. To add your changes to the map, click **Submit**.

Results

Your changes appear on the Location Map portlet when you refresh the portlet page.

Customizing the Location Map Manager portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related concepts:

“Location Map” on page 261

Use the Location Map portlet to see events marked on a location map. A location map in the IBM Intelligent Operations Center is a map or plan with predefined areas for interaction, for example, seating areas in a major sports stadium.

Related reference:

“Location Map Manager portlet settings” on page 149

Customize the Location Map Manager portlet by changing the settings in the fields of the **Shared Settings** window.

Specifying system-wide configuration data

The IBM Intelligent Operations Center system properties table stores IBM Intelligent Operations Center configuration data.

The following properties are system-wide properties used by the IBM Intelligent Operations Center.

Table 63. System-wide values used by the IBM Intelligent Operations Center

| Realm | Subject | Name | Type | Value |
|--------|---------|-----------------------------------|---------|---|
| System | * | ActivityCollectionRefreshInterval | Integer | The collection refresh rate on the server in seconds. The default is 300 (5 minutes). This property affects the UI service rate of refresh for activities. |
| System | * | ActivityProviderEJBNDIName | String | The JNDI binding name of the remote interface of the activity provider. Through this interface, you can deploy your own activity provider to work with your process or workflow management system. The activity provider is an EJB which implements the activity interface in the iss_common.jar. |
| System | * | AppMonitorPort | String | The web port used by Tivoli Monitoring. |
| System | * | ApplicationServerHostname | String | The host name or IP address used by the application server. |
| System | * | CollectionRefreshInterval | Integer | The collection refresh rate on the server in seconds. The default is 15 seconds. This property affects the UI service rate of refresh for events and notifications. |
| System | * | DatabaseServerHostname | String | The host name or IP address used by the data server. |
| System | * | DateFormat | String | The format used when the IBM Intelligent Operations Center displays the date. The default is yyyy-MM-dd. Any valid Java <code>java.text.SimpleDateFormat</code> date pattern can be specified. |
| System | * | DateTimeFormat | String | The format used when the IBM Intelligent Operations Center displays the date and time. The default is yyyy-MM-dd HH:mm:ss. Any valid Java <code>java.text.SimpleDateFormat</code> date and time pattern can be specified. |

Table 63. System-wide values used by the IBM Intelligent Operations Center (continued)

| Realm | Subject | Name | Type | Value |
|--------|---------|------------------------------|---------|--|
| System | * | DisableTSRMSync | Boolean | Specifies whether Tivoli Service Request Manager synchronization is disabled. The default is false. Set to true if a deployment does not contain Tivoli Service Request Manager installation. |
| System | * | EventContainerDeleteEvent | String | Specifies whether an event is deleted from the Object Server database of Tivoli Netcool/OMNIbus. The deletion is implemented by Tivoli Netcool/Impact policy when the IBM Intelligent Operations Center database is updated with an event. The default is true. If the value is true, the event is cleared from the Object Server database. If the value is false, the event is not cleared from the Object Server database. |
| System | * | EventRouterPollDelay | Integer | The delay in milliseconds between UI polling intervals. The delay is the number of milliseconds before the next polling interval. The default is 0. |
| System | * | EventRouterPollErrorDelay | Integer | The delay in milliseconds between UI polling intervals after an error occurs. The delay is the number of milliseconds after an error and before the next polling interval. The default is 5000. |
| System | * | EventRouterTimeout | Integer | The UI polling interval in seconds. The polling interval is the time interval in which to poll for events before timeout. The default is 20. |
| System | * | EventServerHostname | String | The host name or IP address used by the event server. |
| System | * | MgmtServerHostname | String | The host name or IP address used by the management server. |
| System | * | ModelManagerServerEJBPort | String | The EJB port used by semantic model services. |
| System | * | ModelManagerServerHostname | String | The host name or IP address used by semantic model services. |
| System | * | MonitorServerHostname | String | The host name or IP address used by IBM WebSphere Business Monitor. |
| System | * | MonitorServerWebPort | String | The web port used by IBM WebSphere Business Monitor REST Services Gateway. |
| System | * | MonitorServerSecurityEnabled | Boolean | Specifies whether the connection to IBM WebSphere Business Monitor uses SSL for secure HTTP connection. The default is true. If the values is true, the connection uses SSL If the value is false, the connection does not use SSL. |

Table 63. System-wide values used by the IBM Intelligent Operations Center (continued)

| Realm | Subject | Name | Type | Value |
|--------|---------|-----------------------------|--------|---|
| System | * | PortalServerHostname | String | The host name or IP address used by WebSphere Portal Server. |
| System | * | PortalServerWebPort | String | The web port used by the WebSphere Portal Server. |
| System | * | RegExpEmail | System | The regular expression used to validate an email address. The default is .+. |
| System | * | RegExpTelephone | System | The regular expression used to validate a telephone number. The default is .+ |
| System | * | SecurityUserPrefix | String | The user ID prefix used to map the user to the LDAP distinguished name. The default is uid. |
| System | * | SecurityUserSuffix | String | The user ID suffix used to map the user to either an LDAP distinguished name or a local distinguished name. The default, used when running a portal with LDAP security, is ou=users,ou=SWG,o=IBM,c=US. Set the value to o=defaultWIMFileBasedRealm when running a local portal with no LDAP security. |
| System | * | TdsPort | String | The web port used by Tivoli Directory Server Web Administration Tool |
| System | * | TimeFormat | String | The format used when the IBM Intelligent Operations Center displays the time. The default is HH:mm:ss. Any valid Java <code>java.text.SimpleDateFormat</code> time pattern can be specified. |
| System | * | TSRMDirectServerHostname | String | The host name or IP address used by Tivoli Service Request Manager. |
| System | * | TSRMDirectServerWebPort | String | The web port used by Tivoli Service Request Manager. |
| System | * | TSRMServerActivityUri | String | The activity and task application URI used by Tivoli Service Request Manager. The default is <code>/tsrm/maximo/ui/maximo?event=loadapp&value=Activity&uniqueid={0}</code> . The activity ID value is substituted for {0}. |
| System | * | TSRMServerResourceAddUri | | The add resource URI used by Tivoli Service Request Manager. The default is <code>/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=INSERT</code> . The external resource ID value is substituted for {0}. |
| System | * | TSRMServerResourceDeleteUri | | The delete resource URI used by Tivoli Service Request Manager. The default is <code>/tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalevent=useqbe&additionaleventvalue=LOCATION={0}</code> . The external resource ID value is substituted for {0}. |

Table 63. System-wide values used by the IBM Intelligent Operations Center (continued)

| Realm | Subject | Name | Type | Value |
|--------|---------|---------------------------------|---------|---|
| System | * | TSRMServerResourcePropertiesUri | | The resource properties URI used by Tivoli Service Request Manager. The default is /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalEvent=useqbe&additionalEventValue=LOCATION={0}. The external resource ID value is substituted for {0}. |
| System | * | TSRMServerResourceUpdateUri | | The update resource URI used by Tivoli Service Request Manager. The default is /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additionalEvent=useqbe&additionalEventValue=LOCATION={0}. The external resource ID value is substituted for {0}. |
| System | * | TSRMServerSecurityEnabled | Boolean | Specifies whether the HTTP connection to Tivoli Service Request Manager is to use SSL. The default is false. If the value is true, the connection uses SSL If the value is false, the connection does not use SSL. |
| System | * | TSRMServerWorkflowUri | String | The workflow URI used by Tivoli Service Request Manager. The default is /maximo/ui/?event=loadapp&value=sr&&additionalEvent=useqbe&additionalEventValue=TICKETID={0}. The incident ID value is substituted for {0}. |
| System | * | UseDBModelReader | Boolean | Specifies whether the KPI database model is read from an RDF file. The default is true. If the value is true, the KPI model is not read from an RDF file. If the value is false, the KPI model is read from an RDF file. |
| System | * | WebSEALServerHostname | String | The host name or IP address used by Tivoli Access Manager WebSEAL. |

The following properties can be changed to configure how KPIs are processed.

Table 64. Properties affecting KPI processing

| Realm | Subject | Name | Type | Value |
|-------|---------|-----------|---------|--|
| KPI | * | CacheKpis | Boolean | Specifies whether KPIs retrieved from IBM WebSphere Business Monitor are cached. The default is true. If the value is true, KPIs are cached for reuse. How often the cache is refreshed is specified by KpiCacheRefreshInterval. If value is false, KPIs are always retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center requests KPI information. |

Table 64. Properties affecting KPI processing (continued)

| Realm | Subject | Name | Type | Value |
|-------|---------|-------------------------|---------|--|
| KPI | * | KpiCacheRefreshInterval | Integer | Specifies how often the KPI cache is refreshed. The interval is specified in seconds. The default is 300 (5 minutes). KpiCacheRefreshInterval is ignored if CacheKpis is specified as false. |
| KPI | * | KpiSentToGroup | String | Specifies the groups that receive KPI notifications. Separate group names with a semicolon (;). The default value is CityWideExecutive;CityWideSupervisor. |
| KPI | * | PreLoadKpis | Boolean | <p>Specifies whether the KPIs are retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center starts. The default is true.</p> <p>If true, all KPIs are retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center is started. The KPIs are cached for reuse. KpiCacheRefreshInterval specifies how often the cache is refreshed.</p> <p>If false, KPIs are retrieved from IBM WebSphere Business Monitor only when the IBM Intelligent Operations Center requests KPI information.</p> <p>Note: If PreLoadKpis is true, then CacheKpis is assumed to be true regardless of its specified value.</p> |

Updating the system properties table

To change system-wide IBM Intelligent Operations Center configuration data, update the system properties table.

About this task

Use a VNC client to log on to the data server database server and open a command window. In the following procedure, enter commands in the command window.

Procedure

1. Log on to the data server as root
2. To open DB2[®] Control Center, temporarily turn off access control; enter the commands:


```
xhost +
su - db2inst1
db2cc
```
3. In DB2 Control Center, open the system properties table:
 - a. To open DB2 Control Center, enter the following command: `- db2cc`
 - b. In DB2 Control Center, click **All Databases > IOCDB > Tables > SYSPROP**.
 - c. Right-click the **SYSPROP** table, and then click **Open**.
 - d. Modify the required field and click **Commit**
 - e. Close the table.
4. Close DB2 Control Center.
5. To switch back to root user, enter the command: `exit` .
6. To turn access control on again, enter the command: `xhost -`

Note: To implement the changes you made, you must restart the portal server. You can restart the portal server with the IOControl script. For information about starting the services, see the link at the end of this topic.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

Configuring IBM Cognos Business Intelligence to create reports

IBM Intelligent Operations Center provides a reporting subsystem that uses IBM Cognos® Business Intelligence to create and manage reports. The IBM Intelligent Operations Center comes with a reports page that can display up to six reports. You can also create a reports page manually and customize the portlet layout.

The reporting subsystem is installed on the application server and uses an analytic data model.

Creating a Reports portlet

Use the information in this topic to create a Reports portlet page by copying an existing portlet using the IBM Intelligent Operations Center console.

About this task

To copy an existing portlet and set properties to create a new report page, complete the following steps.

Procedure

1. Log on to the IBM Intelligent Operations Center as an administrator.
2. Navigate to **Administration > Portlet Management > Portlets**.
3. In the **Search** field, enter Reports and click **Search**. The Reports portlet window is displayed.
4. Beside the portlet that you want to copy, click the **Copy portlet** icon. The Copy portlet window is displayed.
5. For the name of the new portlet, enter CognosReport.
6. Click **OK**. The new portlet is displayed in the Manage Portlets window.
7. Navigate to **Administration > Portal User Interface > Manage Pages**.
8. Click **Content Root > Citywide** and click the **New Page** tab. The Page Properties page is displayed.
9. Enter the following properties for the new report page:
 - a. In the **Title** field, enter a title for the report page. An example title is Operator: Reports.
 - b. In the **Unique Name** field, enter a name that specifically identifies this report page. An example unique name is com.ibm.iss.ioc.citywide.OperatorReports.
 - c. In the **Friendly URL name** field, enter report.
 - d. In the **Theme** field, accept the default **Inherit Parent Theme**.
 - e. In the **Theme Style** field, accept the default **Inherit Parent Theme Policy**.
 - f. Under **Aggregation-Render Mode**, select **Inherit Parent Render Mode**.
 - g. Click **OK**.

The new report page is added to the list of portlet pages.

Editing the Reports portlet layout

Use these steps to format the layout of your Reports portlet page.

About this task

To select the layout of the Reports portlet page using the IBM Intelligent Operations Center console, complete the following steps.

Procedure

1. Log on to the IBM Intelligent Operations Center as an administrator.
2. Navigate to **Administration > Portal User Interface > Manage Pages**.
3. Next to the page that you want to edit, click the **Edit Page Layout** icon. The Edit Layout page is displayed.
4. Select the layout icon that has side-by-side pages with a row beneath the pages. This icon is the fifth icon from the left.
5. In the frame where you want to add the portlet, click **Add Portlets**.
6. Search for and select the **CognosPortlet** check box and click **OK** to add the portlet to the page layout. A message is displayed confirming that the portlet was added.
7. Repeat steps 5 and 6 to add additional portlets. You can add up to six portlets.
8. Click **Done**.

What to do next

You can edit the shared settings for each portlet. In the top-right corner of the portlet that you want to edit, click the arrow and select **Edit Shared Settings** from the menu. For more information, see “Customizing a portlet to display reports.”

Customizing a portlet to display reports

Use the information in this topic to customize an IBM Intelligent Operations Center portlet to display IBM Cognos Business Intelligence reports.

Procedure

1. Log on to the solution portal as an administrator.
2. Select the view and portlet that you want to customize to display reports.
3. Navigate to the portlet display menu in the upper right corner of the portlet.
4. Click **Edit Shared Settings**.
5. Enter your settings in the fields provided.
 - a. Enter a title for the report.
 - b. Enter the **URL** for the report. Locate the required URL as described in the topic “Locating the report URL” on page 177.

```
Example: CAP_events_by_type_status_and_date:  
http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run  
&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_date%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=true
```
 - c. Set the portal **Width** to *600*.
 - d. Set the portal **Height** to *600*.
 - e. Click **Save**.
 - f. On the portlet display menu, click **Back** to return to the main portlet view.

Results

The Reports portlet updates to display the recently selected report.

Locating the report URL

This topic provides the steps for finding the URL for a report.

Procedure

1. Log on to IBM Cognos Connection.
2. Navigate to **Public Folders > ioc_model > reports**.
3. Select a report and click the **Set properties** icon.
4. On the **General** tab, click **View the search path, ID and URL** to display the report URL.
5. From the **Default action URL** section, copy the URL and paste it into the portlet as required.

Working with the data model

IBM Intelligent Operations Center provides two data models that are used when generating reports. A metamodel defines the language and processes from which to form a model.

Reports in IBM Intelligent Operations Center are built on two data models.

- Common Schema Data Model
- Common Alerting Protocol (CAP) Schema Data Model

Both IBM Intelligent Operations Center data models are organized as layers. For report authors, the Presentation View or layer is made available and consists of the following namespaces:

Business

Contains dictionaries, filters, and data.

Dimensional

Contains event dimensions for reports and analysis.

Custom Query

Contains query subjects that you can use to build custom queries for relational reporting.

Generating the common schema data model reports

This topic describes how to generate the common schema data model reports. These reports help managers and supervisors monitor current events, react to events that are happening, and plan for future events.

About this task

Using the IBM Intelligent Operations Center console, complete these steps to generate common schema data model reports. Refer to the reference links at the end of this topic for a description of the options to generate a report.

Procedure

1. On the IBM Intelligent Operations Center console Administration tab, click **Intelligent Operations > Administration Tools > Administration Consoles**. The Administration Consoles page is displayed.
2. Under Application Server, click **Report Administration**. The IBM Cognos Connection page is displayed.
3. Click **ioc common model**. The Cognos public folders are displayed.
4. Click **Reports**.
5. Select the type of report that you want to generate:
 - To generate a pie chart report, click **Pie charts**. The common schema pie chart reports are displayed.
 - To generate a table chart report, click **Table charts**. The common schema table chart reports are displayed.
6. Select the report that you want to generate.

Pie chart options:

This topic provides the options that you can select for the common pie chart reports.

To access the pie charts reports from the IBM Cognos Connection page, click **Public Folders** > **ioc_common_model** > **reports** > **Pie charts**.

Table 65. Pie chart options for the common schema data model reports

| Report | Description |
|------------------------|---|
| Event by category | Displays events based on event category. For example, you can view all environmental, fire, or transportation events. |
| Event by certainty | Displays events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Event by date sent | This report shows events that were sent on a particular date. |
| Event by event type | Displays events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| Event by headline | Displays events by the description entered for the event when the event was created. Therefore, the headline is actually the event description. |
| Event by severity | Displays events based on severity. For example, events might be extreme or severe. |
| Event by specification | Displays events by specification. For example, an event can be a Common Alerting Protocol or a non-Common Alerting Protocol event. So, this chart shows the percentage of Common Alerting Protocol and non-Common Alerting Protocol events. |
| Event by urgency | Displays events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Event by URL | Displays events by the URL entered for the event when the event was created. |

Table chart options:

This topic describes the information that you can generate for the common table chart reports.

To access table charts reports from the IBM Cognos Connection page, click **Public Folders** > **ioc_common_model** > **reports** > **Table charts**.

The only table chart option for common schema data model reports is Event List. The event list provides a complete list of events with detailed information for each event. Some examples of information on the event list are explained below.

Table 66. Event list information for common table charts

| Report field | Description |
|-------------------|---|
| ID | Identifies the report |
| External event ID | The event ID generated when the event was created. |
| Specification | Specifies if the event is a Common Alerting Protocol or a non-Common Alerting Protocol event. |

Table 66. Event list information for common table charts (continued)

| Report field | Description |
|--------------|--|
| Event type | Displays events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| Sent | The date and time that the event was sent. |
| Headline | The description of the event. |
| Category | Displays events based on event category. For example, you can view all environmental, fire, or transportation events. |
| Certainty | Displays events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Severity | Displays events based on severity. For example, events might be extreme or severe. |
| Urgency | Displays events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Url | The URL associated with the report. |

Generating the Common Alerting Protocol schema data model reports

This topic describes how to generate the Common Alerting Protocol schema data model reports. These reports help managers and supervisors monitor current events, react to events that are happening, and plan for future events.

About this task

Using the IBM Intelligent Operations Center console, complete these steps to generate Common Alerting Protocol schema data model reports. Refer to the reference links at the end of this topic for a description of the options to generate a report.

Procedure

1. On the IBM Intelligent Operations Center console Administration tab, click **Intelligent Operations > Administration Tools > Administration Consoles**. The Administration Consoles page is displayed.
2. Under Application Server, click **Report Administration**. The IBM Cognos Connection page is displayed.
3. Click **ioc cap model**. The Cognos public folders are displayed.
4. Click **Reports**.
5. Select the type of report that you want to generate:
 - To generate a data model report that is listed on this page, select the report.
 - To generate a pie chart report, click **Pie charts**. The common schema pie chart reports are displayed. Select the report from the list.
 - To generate a user-defined report, click **User-defined reports**. The Cognos Custom report page is displayed. Complete the fields for the custom report and click **Update**.

Data model report options:

This topic describes the options that you can select for generating a Common Alerting Protocol report.

To access these report options from the IBM Cognos Connection page, click **Public Folders > ioc_cap_model > reports**.

Table 67. Options for information on the Common Alerting Protocol reports

| Report | Description |
|--|---|
| Common Alerting Protocol events by type, status, and date | This report shows Common Alerting Protocol events by event type, event status, and event date. For example, the event type might be accident and the status might be urgent. The date might be today's date. |
| Common Alerting Protocol events KPI metrics by date | This report shows Common Alerting Protocol events based on KPI metrics for a particular date or range of dates. |
| Common Alerting Protocol events KPI metrics by department | This report shows Common Alerting Protocol events based on KPI metrics for a particular department or area. For example, the report might show KPI metrics for the water department or for a particular area of a city. |
| Common Alerting Protocol full details | This report shows complete details about Common Alerting Protocol events. For example, details include the Common Alerting Protocol ID, sender, the date and time sent, status, message type, source, and others. |
| IBM Intelligent Operations Center events by severity anytime | This report lists all IBM Intelligent Operations Center events based on how severe they are. For example, events might be extreme. |
| IBM Intelligent Operations Center events by severity in progress | This report lists all IBM Intelligent Operations Center events currently happening by severity. For example, the severity in progress might be extreme weather that is occurring. |

Pie chart options:

This topic describes the options you have for generating Common Alerting Protocol pie chart reports.

To access the pie chart reports from the IBM Cognos Connection page, click **Public Folders > ioc_cap_model > reports > Pie charts**.

Table 68. Options for information on Common Alerting Protocol pie chart reports

| Report | Description |
|----------------------|---|
| Cap by category | Displays Common Alerting Protocol by a particular category. For example, you can view all environmental, fire, or transportation events. |
| Cap by certainty | Displays Common Alerting Protocol events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Cap by date sent | Displays Common Alerting Protocol events sent on a particular date. |
| Cap by event type | Displays Common Alerting Protocol events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| Cap by handling code | Displays Common Alerting Protocol events by handling code. For example, the handling code might be "event." |
| Cap by message type | Displays Common Alerting Protocol events based on message types such as updates and alerts. |
| Cap by scope | Displays Common Alerting Protocol events by scope. For example, an event by scope might be "public." |

Table 68. Options for information on Common Alerting Protocol pie chart reports (continued)

| Report | Description |
|--------------------------|--|
| Cap by sender | Displays Common Alerting Protocol events by the sender's name. |
| Cap by severity | Displays Common Alerting Protocol events based on severity. For example, events might be extreme or severe. |
| Cap by source | Displays Common Alerting Protocol by a particular source. For example, the source might be transportation. |
| Cap by status | Displays Common Alerting Protocol events by status. The statuses are: <ul style="list-style-type: none"> • Acceptable • Caution • Take action |
| Cap by urgency | Displays Common Alerting Protocol events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Notification by category | Displays alert messages in Common Alerting Protocol format by a particular category. For example, you can view all environmental, fire, or transportation events. |
| Notification by type | Displays notifications in Common Alerting Protocol format by type. For example, the type might be updates and alerts. |

User-defined events reports options:

This topic describes the options you have for generating Common Alerting Protocol user-defined reports for events.

To access the user-defined reports from the IBM Cognos Connection page, click **Public Folders** > **ioc_cap_model** > **reports** > **User-defined reports** > **Events**.

Table 69. Common Alerting Protocol events options

| Report | Description |
|------------------------------|---|
| Events by Category Anytime | Displays all events by category regardless of date. For example, you can view all environmental, fire, or transportation events. |
| Events by Certainty Anytime | Displays all events by certainty regardless of date. For example, if a traffic accident occurred, the certainty might be "observed." |
| Events by Event Type Anytime | Displays all events by event type regardless of date. For example, events might be a tornado approaching or a traffic accident that occurred on any date. |
| Events by Severity Anytime | Displays all events by severity regardless of date. For example, extreme or severe events for any date are displayed. |
| Events by Urgency Anytime | Displays all events by urgency regardless of date. For example, events might be occurring and described as "immediate." |

User-defined custom report options:

This topic describes the options you have for generating Common Alerting Protocol user-defined custom reports.

You can create a custom report for events using the Reports portlet. Begin by selecting how you want to group events. For example, to view all events by a particular category, select **Category** in the **Group by** field. Then in the **Select data** fields, choose the data specific to the information that you want to view. You can also indicate a date or range of dates for the events on the report. Click **Update**, and the graph changes to reflect the information you requested.

To retrieve the URL for the new report, click **URL For This Report**.

To access the custom user-defined reports from the IBM Cognos Connection page, click **Public Folders > ioc_cap_model > reports > User-defined_reports > User-defined report**.

Table 70. Common Alerting Protocol user-defined custom options

| Report | Description |
|----------------|--|
| Group by | Select the option that you want to group events by. |
| Severity | Displays events based on severity. For example, events might be extreme or severe. |
| Certainty | Displays events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Urgency | Displays events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Event Category | Displays events based on event category. For example, you can view all environmental, fire, or transportation events. |
| Event Type | Displays events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| From Date | Enter the date for which you are viewing events. For a range of dates, enter the beginning date. |
| To Date | Enter the date through which you are viewing events. |

Configuring common schema data model reports

Use this topic to set general and specific properties for common schema data model reports.

Before you begin

You must have Administrator access to perform this procedure.

About this task

Use the IBM Intelligent Operations Center console to configure these reports.

Procedure

1. On the IBM Intelligent Operations Center console Administration tab, click **Intelligent Operations > Administration Tools > Administration Consoles**. The Administration Consoles page is displayed.
2. Under Application Server, click **Report Administration**. The IBM Cognos Connection page is displayed.

3. Select the **ioc common model** check box, and then click **More**. The Available actions page is displayed.
4. Click **Set properties**. The General properties page is displayed.
5. Select the values for the general report properties.
6. On the Permissions tab, select the permissions for the common schema data model reports.
7. On the Capabilities tab, select the capabilities for the reports.
8. Click **OK**.

Configuring Common Alerting Protocol schema data model reports

Use this topic to set general properties, set permissions, and assign capabilities to types of users for Common Alerting Protocol schema data model reports.

Before you begin

You must have Administrator access to perform this procedure.

About this task

Use the IBM Intelligent Operations Center console to configure these reports.

Procedure

1. On the IBM Intelligent Operations Center console Administration tab, click **Intelligent Operations > Administration Tools > Administration Consoles**. The Administration Consoles page is displayed.
2. Under Application Server, click **Report Administration**. The IBM Cognos Connection page is displayed.
3. Select the **ioc cap model** check box, and then click **More**. The Available actions page is displayed.
4. Click **Set properties**. The General properties page is displayed.
5. Select the values for the general report properties.
6. On the Permissions tab, select the permissions for the Common Alerting Protocol schema data model reports.
7. On the Capabilities tab, select the capabilities for the users of the reports.
8. Click **OK**.

More reports options

This topic describes additional report options for both common and Common Alerting Protocol reports.

To access these options, click **More** to the right of the link for a particular report.

Table 71. Additional options available for each report

| Option | Description |
|-------------------------------------|--|
| Set properties | Set general properties for the report you choose. |
| View report output version | Choose the output version to view by clicking a format hyperlink. |
| View my permissions | View the access permissions you have for this entry. |
| Run with options | Select how you want to run and receive your report. Examples include HTML and PDF. |
| Open with Report Studio | Displays the report in another browser using Report Studio. |
| Open with Business Insight Advanced | Displays the report in another browser using IBM Cognos Business Insight Advanced. |
| New schedule | Schedules a report based on various criteria. |

Table 71. Additional options available for each report (continued)

| Option | Description |
|-------------------------------------|---|
| Move | Moves a report to a different location. |
| Copy | Copies a report from one location to another. |
| Create a shortcut to this entry | Creates a shortcut on your desktop for accessing the report. |
| Create a report view of this report | Creates a view on your desktop for this report that is stored in a local directory. |
| Delete | Deletes a report that is displayed. |

Chapter 6. Managing the solution

The topics in this section describe how to perform administrative tasks for IBM Intelligent Operations Center.

About

Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation.

To launch the About portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > About**.

The About portlet supplies the following information:

- The location of all installed software products and components
- The name and version of the products installed
- The name and version of the components installed
- The details of any fixes applied

The components that are identified are components or portions of a product, for example:

- A portion of a product that has a dedicated maintenance or service stream
- An optionally installable portion of a product
- Portions of a product that are shared by multiple products

Note: The information displayed for each fix depends on completion of the appropriate step in the installation instructions supplied with that fix.

Customizing the About portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related tasks:

“Verifying the installation” on page 48

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

Related reference:

“About portlet settings” on page 139

Customize the About portlet by changing the settings in the fields of the **Shared Settings** window.

Controlling the services

The IBM Intelligent Operations Center services running on the IBM Intelligent Operations Center servers can be controlled and queried.

Starting the services

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

About this task

The **IOCControl.sh** command must be run as the root or `ibmadmin` user. If not logged on as the root or `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Attention: Starting individual services should only be done by experienced IBM Intelligent Operations Center administrators. Unpredictable results can occur if services are not started in the required order.

Procedure

On the management server run the following command to start all the IBM Intelligent Operations Center services.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start all password
```

where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

The services are started in the required order. Prerequisite services are started before dependent services. For example, database and directory services are started first.

To start only one service, run the following command.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start service_ID password
```

where *service_ID* is an ID listed under **Target Options** in the **IOCControl** help and where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

Results

The requested IBM Intelligent Operations Center services are started.

What to do next

After running the **IOCControl.sh** command, check the logs in the `/opt/IBM/ISP/mgmt/logs` directory. The logs contain the results of the **IOCControl.sh** command.

Related tasks:

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Querying the status of the services” on page 191

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

“Getting help for the Platform Control Tool” on page 192

Information is available about the action and target options for the Platform Control Tool.

“Verifying the installation” on page 48

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

“Installing the Platform Control Tool” on page 46

The Platform Control Tool is used to manage the IBM Intelligent Operations Center server environment. The tool is installed separately from the product.

“Installing the System Verification Check tool” on page 47

The System Verification Check tool is used to verify the operational status of components in IBM Intelligent Operations Center. The tool is installed separately from the product.

Required start order

IBM Intelligent Operations Center services must be started in a specific order.

The Platform Control Tool is used to start IBM Intelligent Operations Center services. While it is recommended that the Platform Control Tool **start all** option be used to start all services, there might be times when individual services need to be started.

Some services have dependencies on other services, so services must be started in a specific order.

In general, services should be started in three groups:

Group 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24so1, db24mgmt

Group 2

ihs, appdmgr, st

Group 3

all remaining services

Start the services in group 1 first, then start group 2, and finally group 3. The services within each group can be started in any order.

Table 72. IBM Intelligent Operations Center service start order dependencies

| Service | Description | Services that must be running before this service is started |
|-----------|---|--|
| db24po | DB2 Enterprise Server Edition for WebSphere Portal Server | None |
| db24wbm | DB2 Enterprise Server Edition for WebSphere Business Modeler | None |
| db24so1 | DB2 Enterprise Server Edition for IBM Intelligent Operations Center | None |
| db24ana | DB2 Enterprise Server Edition for Cognos | None |
| db24mgmt | DB2 Enterprise Server Edition for Tivoli Enterprise Portal services | None |
| db24tsrm | DB2 Enterprise server for Tivoli Service Request Manager | None |
| db24sms | DB2 Enterprise server for semantic model services | None |
| tds | Tivoli Directory Server | None |
| tdspxyapp | Tivoli Directory Server Proxy (application server) | tds |
| tdspxyevt | Tivoli Directory Server Proxy (event server) | tds |
| tdspxymgt | Tivoli Directory Server Proxy (management server) | tds |
| tdsappsrv | Tivoli Directory Server Application Server | None |
| tamps | Tivoli Access Manager Policy Server | tamas |
| tamas | Tivoli Access Manager Authorization Server | tds |
| tamwpm | Tivoli Access Manager Web Portal Manager | None |
| tamweb | Tivoli Access Manager WebSEAL | tamas |
| tems | Tivoli Monitoring Enterprise Monitoring Server | None |
| teps | Tivoli Monitoring Enterprise Portal Server | tems, db24mgmt |
| tim | Tivoli Identity Manager | tds |
| appdmgr | WebSphere Application Server Network Deployment | None |
| cplex | WebSphere Application Server for CPLEX | db24sms |
| ihs | HTTP Server for Runtime (application server) | None |
| ihsevt | HTTP Server for Runtime (event server) | ihs |

Table 72. IBM Intelligent Operations Center service start order dependencies (continued)

| Service | Description | Services that must be running before this service is started |
|---------|---|--|
| ihsmt | HTTP Server for Runtime (management server) | ihs |
| ncob | Tivoli Netcool/OMNIBus | None |
| nci | Tivoli Netcool/Impact | ncob |
| wbm | IBM WebSphere Business Monitor | db24wbm |
| st | Lotus Sametime | None |
| stpxy | Lotus Sametime Proxy Application Server | st |
| wpe | WebSphere Portal Extend | tdspxyapp, db24po, appdmgr |
| wmb | WebSphere Message Broker | None |
| cognos | IBM Cognos Business Intelligence | db24ana, appdmgr |
| tsrm | Tivoli Service Request Manager | appdmgr, db24tsrm |
| wodm | WebSphere Operations Decision Manager | appdmgr |
| wodmdc | WebSphere Operations Decision Manager (Decision Center) | None |
| smsclt | Semantic model services (Client Services) | appdmgr |
| smsdaaq | Semantic model services (Data Services) | appdmgr |
| smsmdl | Semantic model services (Model Services) | appdmgr |
| smsgmt | Semantic model services (Management Services) | appdmgr |
| smsrtc | Semantic model services (RTC Services) | appdmgr |
| iocxml | IBM Intelligent Operations Center XML probe | db24sol |

Starting and stopping the Tivoli Netcool/OMNIBus probe

Start the Tivoli Netcool/OMNIBus probe after all IBM Intelligent Operations Center servers have been started.

About this task

The probe is part of the IOControl script. The probe is started and stopped when you start and stop Tivoli Netcool/OMNIBus. The Tivoli Netcool/OMNIBus probe is linked with Tivoli Netcool/OMNIBus in the script. Use the following procedure to stop, start, and verify the status of the probe.

Procedure

- To stop the probe, on the management server run:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop ncob password
```
- To start the probe, on the management server run:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start ncob password
```
- To verify the status of the probe:
 - On the management server, run the command:


```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start iocxml password
```
 - On the event server, run the command:


```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Stopping the services

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

About this task

The **IOCControl.sh** command must be run as the root or `ibmadmin` user. If not logged on as the root or `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Attention: Stopping individual services should only be done by experienced IBM Intelligent Operations Center administrators. Unpredictable results can occur if services are not stopped in the required order.

Procedure

On the management server run the following command to stop all the IBM Intelligent Operations Center services.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop all password
```

where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

To stop only one service, run the following command.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop service_ID password
```

where *service_ID* is an ID listed under **Target Options** in the **IOCControl** help and where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

Results

The requested IBM Intelligent Operations Center services are stopped.

What to do next

After running the **IOCControl.sh** command, check the logs in the `/opt/IBM/ISP/mgmt/logs` directory. The logs contain the results of the **IOCControl.sh** command.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Querying the status of the services” on page 191

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

“Getting help for the Platform Control Tool” on page 192

Information is available about the action and target options for the Platform Control Tool.

“Verifying the installation” on page 48

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

“Installing the Platform Control Tool” on page 46

The Platform Control Tool is used to manage the IBM Intelligent Operations Center server environment. The tool is installed separately from the product.

“Installing the System Verification Check tool” on page 47

The System Verification Check tool is used to verify the operational status of components in IBM Intelligent Operations Center. The tool is installed separately from the product.

Required stop order

IBM Intelligent Operations Center services must be stopped in a specific order.

The Platform Control Tool is used to stop IBM Intelligent Operations Center services. While it is recommended that the Platform Control Tool **stop all** option be used to stop all services, there might be times when individual services need to be stopped.

Some services have dependencies on other services, so services must be stopped in a specific order.

In general, services should be stopped in three groups:

Group 1

tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24so1, db24mgmt

Group 2

ihs, appdmgr, st

Group 3

all remaining services

Stop the services in group 3 first, then stop group 2, and finally group 1. The services within each group can be stopped in any order.

Table 73. IBM Intelligent Operations Center service stop order dependencies

| Service | Description | Services that must be stopped before this service is stopped |
|------------|---|--|
| db24po | DB2 Enterprise Server Edition for WebSphere Portal Server | wpe |
| db24wbm | DB2 Enterprise Server Edition for WebSphere Business Modeler | wbm |
| db24so1 | DB2 Enterprise Server Edition for IBM Intelligent Operations Center | iocxml |
| db24ana | DB2 Enterprise Server Edition for Cognos | cognos |
| db24mgmt | DB2 Enterprise Server Edition for Tivoli Enterprise Portal services | teps |
| db24tsrm | DB2 Enterprise server for Tivoli Service Request Manager | tsrm |
| db24sms | DB2 Enterprise server for semantic model services | cplex |
| tds | Tivoli Directory Server | tdsprxyapp, tdspxyevt, tdspxygmt, tamas, tim |
| tdsprxyapp | Tivoli Directory Server Proxy (application server) | wpe |
| tdspxyevt | Tivoli Directory Server Proxy (event server) | None |
| tdspxygmt | Tivoli Directory Server Proxy (management server) | None |
| tdsappsrv | Tivoli Directory Server Application Server | None |
| tamps | Tivoli Access Manager Policy Server | None |
| tamas | Tivoli Access Manager Authorization Server | tamps |
| tamwpm | Tivoli Access Manager Web Portal Manager | None |
| tamweb | Tivoli Access Manager WebSEAL | None |
| tems | Tivoli Monitoring Enterprise Monitoring Server | teps |
| teps | Tivoli Monitoring Enterprise Portal Server | None |
| tim | Tivoli Identity Manager | None |
| appdmgr | WebSphere Application Server Network Deployment | wpe, cognos, tsrm, wodm, smsclt, smsdaaq, smsmdl, smsrtc, smsgmt |
| cplex | WebSphere Application Server for CPLEX | None |
| ihs | HTTP Server for Runtime (application server) | ihsevt, ihsmgt |
| ihsevt | HTTP Server for Runtime (event server) | None |
| ihsmgt | HTTP Server for Runtime (management server) | None |

Table 73. IBM Intelligent Operations Center service stop order dependencies (continued)

| Service | Description | Services that must be stopped before this service is stopped |
|---------|---|--|
| ncob | Tivoli Netcool/OMNIBus | nci |
| nci | Tivoli Netcool/Impact | None |
| wbm | IBM WebSphere Business Monitor | None |
| st | Lotus Sametime | stpxy |
| stpxy | Lotus Sametime Proxy Application Server | None |
| wpe | WebSphere Portal Extend | None |
| wmb | WebSphere Message Broker | None |
| cognos | IBM Cognos Business Intelligence | None |
| tsrm | Tivoli Service Request Manager | None |
| wodm | WebSphere Operations Decision Manager | None |
| wodmhc | WebSphere Operations Decision Manager (Decision Center) | None |
| smsclt | Semantic model services (Client Services) | None |
| smsdaaq | Semantic model services (Data Services) | None |
| smsmdl | Semantic model services (Model Services) | None |
| smsgmt | Semantic model services (Management Services) | None |
| smsrtc | Semantic model services (RTC Services) | None |
| iocxml | IBM Intelligent Operations Center XML probe | None |

Querying the status of the services

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

About this task

The **IOControl.sh** command must be run as the root or ibmadmin user. If not logged on as the root or ibmadmin, run the **su - ibmadmin** command to switch to the ibmadmin user.

Procedure

On the management server run the following command to query the status all the IBM Intelligent Operations Center services.

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

where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

To check only one service, run the following command.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status service_ID password
```

where *service_ID* is an ID listed under **Target Options** in the **IOControl** help and where *password* is the password for the Platform Control Tool defined when the Platform Control Tool was installed.

Results

Services that are started will display **[on]**. Services that are not started will display **[off]**.

What to do next

After running the **IOControl.sh** command, check the logs in the `/opt/IBM/ISP/mgmt/logs` directory. The logs contain the results of the **IOControl.sh** command.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Getting help for the Platform Control Tool”

Information is available about the action and target options for the Platform Control Tool.

“Installing the Platform Control Tool” on page 46

The Platform Control Tool is used to manage the IBM Intelligent Operations Center server environment. The tool is installed separately from the product.

Getting help for the Platform Control Tool

Information is available about the action and target options for the Platform Control Tool.

About this task

The **IOControl.sh** command must be run as the root or `ibmadmin` user. If not logged on as the root or `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Procedure

On the management server run the one of the following commands to see options for the **IOControl** command.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh help
```

or

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh
```

Results

The options for the **IOControl** command are displayed.

Related tasks:

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Querying the status of the services” on page 191

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

Administration Consoles

Use the Administration Consoles portlet to administer the services provided by the solution.

To access the Administration Consoles portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Administration Tools > Administration Consoles**.

For each service, links in the Administration Consoles portlet direct you either to an administration console, or to information about how to access administration.

Note: If you are using Microsoft Internet Explorer version 8.0, you might encounter a problem with the report administration link. The message is: Cannot find the resource you have requested. The solution is to edit the URL in the browser address field by adding, /cognos, between the hostname and /ServletGateway.

Application server

Table 74. Administration on the application server

| Console | Administration |
|-----------------------|---|
| Application server | To administer various services provided by the IBM Intelligent Operations Center, use the link to the web-based console for WebSphere Application Server. You can control the servers, manage resources and service providers, change host and other environmental settings. |
| Report administration | To set up reports, use the link to the web-based console for IBM Cognos Connection. You can create new 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

Table 75. Administration on the data server

| Console | Administration |
|----------|---|
| Database | For details on 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. |

Event server

Table 76. Administration on the event server

| Console | Administration |
|--------------------------------|---|
| Contacts | To view current settings in the names.nsf database, use the link to the web-based console for Lotus Domino Server. names.nsf is used to configure Lotus Domino Server. Configuration changes can be made with Domino Administration Client. |
| Contacts administration | For details on how to download and set up Domino Administration Client for Lotus Domino contacts administration, use the link to the information center. |
| Event handling | To administer event handling with the object server GUI, use the link to the web-based console for Tivoli Netcool/OMNIBus. |
| Event processing and enhancing | To administer event processing, use the link to the web-based console for Tivoli Netcool/Impact. For example, you can check database connections, data source connections, event process initiation, policy status, and logs. |

Table 76. Administration on the event server (continued)

| Console | Administration |
|---|--|
| Instant messaging server | To administer instant messaging, use the link to the web-based console for Lotus Sametime Community Server. |
| Message bus | For details on how to check message status with WebSphere Message Broker, use the link to the information center. |
| Standard operating procedure administration | To define resources and standard operating procedures, use the link to the web-based console for Tivoli Service Request Manager Start Center. You can define available resources and activities for event management in the IBM Intelligent Operations Center. |
| Standard operating procedure application server | To administer, use the link to the web-based console for WebSphere Application Server which serves Tivoli Service Request Manager. |

Management server

Table 77. Administration on the management server

| Console | Administration |
|-----------------------------------|---|
| Application monitoring | To administer application monitoring, use the link to the web-based console for Tivoli Monitoring. You can work with this console for system health checks. |
| Application server for management | To administer integrated applications, use the link to the web-based console for WebSphere Application Server. This administration includes security administration with Tivoli Access Manager and WebSEAL. |
| Database | For details on 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 | To administer the user's directory, link to the web-based console for Tivoli Directory Server. For details on how to use the Tivoli Directory Server web-based console, use the link to the information center. |

Customizing the Administration Consoles portlet

You can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Related reference:

“Administration Consoles portlet settings” on page 140
Customize the Administration Consoles portlet by changing the settings in the fields of the **Shared Settings** window.

Related information:

 [IBM Lotus Domino and Notes information center](#)

 [IBM DB2 Database information center](#)

 [IBM Tivoli Directory Server information center](#)

Managing the services

The Administration Consoles portlet provides links to locations where you can manage the services provided by the solution, or find more detailed information about managing the services.

Application server

Application server service

You can perform a wide variety of application management tasks on a common web-based console, the Integrated Solutions Console:

- Check the status of servers.
- Start and stop servers and clusters.
- Deploy applications or patches.
- Manage the list of available portlets.
- Monitor the services.
- Work with application service policies.
- Manage service providers, including REST service providers.
- Manage resources.
- Manage the security of your applications.
- Work with virtual hosts and other environmental settings.
- Perform system administration.
- Manage service integration.
- Administer the HTTP Server.
- Manage logging and tracing.

For more information about the application service, see the online help for the Integrated Solutions Console, or see the link to the WebSphere Application Server information center at the end of the application server section.

Report administration service

For all the tasks associated with providing reports within the IBM Intelligent Operations Center, you can use the web-based report administration console:

- Set up data sources.
- Create, edit, and delete reports.
- Manage access to reports.
- Schedule reports.
- Set up the distribution of reports.

For more information about the report administration service, see the link to the IBM Cognos Business Intelligence information center at the end of the application server section.

Related information:

 [WebSphere Application Server Version 7.0 information center](#)

 [IBM Cognos Business Intelligence information center](#)

Data server

Database service

You can manage the IBM Intelligent Operations Center databases through the database service instances hosted on the data server. A database service instance is a separate, independent process that runs on a server. An instance can host multiple databases. Each instance has a name *instance-name*. The following instances are hosted on the data server:

Table 78. Database instances hosted on the data server

| Instance | Used by |
|----------|---|
| dsrdbm01 | directory service |
| db2inst1 | reserved for solutions |
| db2inst2 | portal server |
| db2inst3 | report administration |
| db2inst4 | business rules and business monitoring service |
| db2inst5 | semantic model services |
| db2inst6 | standard operating procedure administration service |
| db2inst7 | identity management service |
| db2inst8 | reserved for applications |

To administer an instance from a terminal window:

1. Log in as the *instance-name* user.
2. Run the command **db2** to enter command mode.
3. Enter **?** to see a list of available commands. Many commands require an active connection to a database.
 - To see the available databases for an instance, run the command **list database directory**.
 - To connect to a database, run the command **connect to database_name**.
4. To disconnect from a database and end the prompted command mode, run the command **terminate**.

For more information about the database service, see the link to the DB2 Database information center at the end of the data server section.

Related information:

 [IBM DB2 Database information center](#)

Event server

Contacts, contacts administration, and instant messaging services

You can manage contacts, contacts administration, instant messaging services through:

- Lotus Domino Server console to view your current contacts.
- Lotus Domino Administration Client to configure single sign-on, administer the instant messaging server, and the Lotus Sametime Client.

- Lotus Sametime Community Server to log and check the availability of the instant messaging server.

Note: Contacts viewed on the Lotus Domino Server console apply to the Contacts portlet only and are not the same as IBM Intelligent Operations Center users.

For more information about the contacts, contacts administration, and instant messaging services, see the link to the Lotus Domino and Notes information center at the end of the event server section.

Event handling service

You can manage event capture and storage in the IBM Intelligent Operations Center through the Tivoli Netcool/OMNIbus object server GUI.

1. Open an X Window System enabled terminal session.
2. Log on as root on the server.
3. Go to the `/opt/IBM/netcool/omnibus` directory.
4. To open the GUI application, run the command: `bin/nco_config`

For more information about the event handling service, see the link to the Tivoli Netcool/Impact information center at the end of the event server section.

Event processing and enhancing service

You can manage event processing, through the web-based console for Tivoli Netcool/Impact:

- Check the database and data source connections.
- Check that the EventProcessor is running.
- Check logging for existing policies and update log level.
- Update existing policies, or create new policies.

For more information about the event processing and enhancing service, see the link to the Tivoli Netcool/Impact information center at the end of the event server section.

Message bus

The three main methods for managing the message bus service are:

- Command line
- Explorer: an Eclipse-based administrative application
- Toolkit: an Eclipse-based application that allows both administration and application development

You can manage communication flows, define tests, transformations, integrations, and logging, with the GUI development tool.

The WebSphere Message Broker Toolkit is provided with the IBM Intelligent Operations Center. For information on installing and using the toolkit, see the link to the WebSphere Message Broker information center at the end of the event server section

To set up the command-line environment and query WebSphere Message Broker instances:

- Log on to the server as user `mqm`.
- Go to the `/opt/IBM/mqsi/8.0.0.0` directory.
- To set up the environment, run the command `source bin/mqsiprofile`.
- To query WebSphere Message Broker instances, run the command: `bin/mqsilist`.

For more information about the message bus service, see the link to the WebSphere Message Broker information center at the end of the event server section.

Standard operating procedure administration service

You can define resources and activities to manage events through the web-based standard operating procedure administration console, Tivoli Service Request Manager start center.

For more information about the standard operating procedure administration service, see the Tivoli Service Request Manager information center link at the end of the event server section.

Standard operating procedure application service

You can manage applications associated with resources and activities through the web-based console for WebSphere Application Server, which serves Tivoli Service Request Manager.





For more information about the standard operating procedure application service, see the online help, or see the link to the WebSphere Application Server Version 7.0 information center at the end of the application server section.

Related concepts:

“Configuring Tivoli Service Request Manager” on page 119

In the Tivoli Service Request Manager user interface, you can manage standard operating procedures, workflows, and resources.

Related information:

-  [IBM Lotus Domino and Notes information center](#)
-  [IBM Tivoli Netcool/Impact information center](#)
-  [IBM WebSphere Message Broker information center](#)
-  [IBM Tivoli Service Request Manager information center](#)

Management server Application monitoring service

You can manage application monitoring through the web-based console for Tivoli Monitoring. Download the application and run it to check the status of the servers and see all the monitoring agents that are running. To log on, enter your user ID and password. The default user ID is sysadmin and the topology password entered during installation.

For more information about the application monitoring service, see the link to the Tivoli Enterprise Portal User's Guide at the end of the topic.

Application server for management service

You can manage junctions for Tivoli Access Manager WebSEAL on the common web-based console, the Integrated Solutions Console.

For more detailed information about this service, see the online help or see the link to the WebSphere Application Server Version 7.0 information center at the end of the application server section.

Database service

There is one database service instance, db2inst2, hosted on the management server. You can use this instance for system management and specific data storage for Tivoli Access Manager.

For more detailed information about the database service, see the link to the IBM DB2 Database information center at the end of the data server section.

Directory service

Manage the users directory through the web-based console for Tivoli Directory Server, you can view, add, or change users in LDAP.

For more detailed information about the directory service, see the link to the Tivoli Directory Server information center, at the end of this topic.

Related information:



IBM Tivoli Monitoring, Tivoli Enterprise Portal user's guide



IBM Tivoli Directory Server information center

Verifying the components

The System Verification Check tool tests components within IBM Intelligent Operations Center to determine if they are accessible and operational.

How to use the System Verification Check tool

The System Verification Check tool is used to determine the operational status of services comprising the IBM Intelligent Operations Center system.

About this task

The System Verification Check tool verifies system capabilities.



For details on individual tests and troubleshooting if the tests fails, click **Help** for the test.

Properties provides additional information about the test for use when calling IBM Software Support.

Procedure

1. Log on to IBM Intelligent Operations Center as a user with administrator authority.
2. Click **Intelligent Operations > Administration Tools > System Verification Check**.
3. Select the test or tests to be run by doing one of the following:
 - Click a specific test to be run.
 - Click **Run All Tests** to test the capabilities of all selections.

Results

The  icon will be displayed when a test completes successfully. The  icon will be displayed when a test fails. If a test fails, follow the problem determination instructions for the test to resolve the errors.

These instructions can also be accessed by clicking the  icon or **Help**.

If a specific test was run, the run results of the test are displayed at the bottom of the portlet along with the test execution time. If **Run All Tests** was selected, this information is not displayed.

What to do next

The tool can be reset, and all results cleared, by clicking **Reset**.

Related tasks:

“Verifying the installation” on page 48

After installing IBM Intelligent Operations Center, verify that the product has been correctly installed.

“Installing the System Verification Check tool” on page 47

The System Verification Check tool is used to verify the operational status of components in IBM Intelligent Operations Center. The tool is installed separately from the product.

System Verification Check tests

IBM Intelligent Operations Center provides a number of System Verification Check tests that can be used to determine the operational status of various IBM Intelligent Operations Center services and components.

The tests are logically grouped by function. For example, collaboration and monitoring.

Account Management (Tivoli Identity Manager API) Test

The Account Management (Tivoli Identity Manager API) test tests access to the Tivoli Identity Manager API by accessing the IIOP port.

Resources

The Account Management (Tivoli Identity Manager API) test uses the following resource:

- Tivoli Identity Manager Server (on the management server).

Problem determination

If the Account Management (Tivoli Identity Manager API) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the management server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the management server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the management server review the following Tivoli Identity Manager logs:
 - `/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. Verify that the file systems on the application server and management server have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the Tivoli Identity Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the management server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the `nodeagent` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Skip this step if message `ADMU0508I: The`

Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

- a. If message ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped. is displayed, start timServer1 using the following command: /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1. Skip this step if message ADMU0508I: The Application Server "timServer1" is STARTED. is displayed. If you had to start timServer1, a message similar to the following will be displayed: ADMU3000I: Server timserver open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. timServer1

Stop servers in this order:

- a. timServer1
- b. nodeagent


The timServer1 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the management server: /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the Tivoli Identity Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at http://MANAGEMENT_SERVER_HOST:9060/admin using the WebSphere Application Server Administrative ID admin and password. *MANAGEMENT_SERVER_HOST* is the host name for the management server.
 - b. View the status of the timServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. timServer1

Stop servers in this order:

- a. timServer1

b. nodeagent

To stop the timServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the management server: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

6. Verify that the Tivoli Identity Manager console can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. Where the `MANAGEMENT_SERVER_HOST` is host name for the management server. Log on with the user ID `itim manager`.

What to do next

Resolve any issues or errors found and retry the test.

Account Management (Tivoli Identity Manager Console) Test

The Account Management (Tivoli Identity Manager Console) test determines if the Tivoli Identity Manager is accessible by accessing the Tivoli Identity Manager Administration URL.

Resources

The Account Management (Tivoli Identity Manager Console) test uses the following resource:

- Tivoli Identity Manager Server (on the management server)

Problem determination

If the Account Management (Tivoli Identity Manager Console) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the management server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the management server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the management server review the following Tivoli Identity Manager logs:
 - `/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. Verify that the file systems on the application server and management server have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the Tivoli Identity Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the management server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Skip this step if message `ADMU0508I: The`

Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

- a. If message ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped. is displayed, start timServer1 using the following command: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Skip this step if message ADMU0508I: The Application Server "timServer1" is STARTED. is displayed. If you had to start timServer1, a message similar to the following will be displayed: ADMU3000I: Server timserver open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. timServer1

Stop servers in this order:

- a. timServer1
- b. nodeagent


The timServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the management server: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the Tivoli Identity Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at `http://MANAGEMENT_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID admin and password. `MANAGEMENT_SERVER_HOST` is the host name for the management server.
 - b. View the status of the timServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. timServer1

Stop servers in this order:

- a. timServer1

b. nodeagent

To stop the timServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the management server: `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

6. Verify that the Tivoli Identity Manager console can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`. Where the `MANAGEMENT_SERVER_HOST` is host name for the management server. Log on with the user ID `itim manager`.

What to do next

Resolve any issues or errors found and retry the test.

Account Management (Tivoli Directory Integrator list assembly) Test

The Account Management (Tivoli Directory Integrator list assembly) test determines if the Tivoli Directory Integrator List Assembly resources are available. To do this the `tdisrvctl` command, which remotely manages configurations, assembly lines, and other functions, is run on the management server and the test looks for the `--- AssemblyLines ---` to be returned.

Resources

The Account Management (Tivoli Directory Integrator list assembly) test uses the following resources:

- Tivoli Directory Server (on the data server)
- Tivoli Directory Integrator (on the management server)

Problem determination

If the Account Management (Tivoli Directory Integrator list assembly) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the data server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the data server and application server systems have not reached capacity. This can be determined using the `df -h` command.
4. Verify that the Tivoli Directory Integrator Server is running.
 - a. Log on a terminal session on the management server as `ibmadmin`.
 - b. Run the `ps -ef | grep ibmdisrv` command. The results will be similar to the following:

```
ibmadmin      11411      1  0 Sep06 pts/1      00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timsol -c ITIM_RMI.xml -d
ibmadmin      32080 19149  0 23:17 pts/1      00:00:00 grep ibmdisrv
```

This example shows that the Tivoli Directory Integrator Server daemon, `ibmdisrv`, is running.
5. Start the Tivoli Directory Integrator Server, `ibmdisrv`, if it is not running.
 - a. Log on a terminal session on the management server as `root`.
 - b. Run `/etc/init.d/ITIMAd start`.
6. Verify that the Tivoli Directory Server LDAP server is running.

- a. Log on to a terminal session on the data server as root.
- b. Run the **ps -ef | grep ibmslapd** command. The results will be similar to the following:

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149    0 23:17 pts/1    00:00:00 grep ibmslapd
```

This example shows that the Tivoli Directory Server daemon, `ibmslapd`, is running.

- c. Run the **ps -ef | grep ibmdiradm** command. The results will be similar to the following:

```
root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

This example shows that the Tivoli Directory Server daemon, `ibmdiradm`, is running.

7. If the Tivoli Directory Server, `ibmslapd`, is not running, do the following.
 - a. As a `root` Linux user, run **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** to start the Directory Server
8. If the Tivoli Directory Administration Server, `ibmdiradm`, is not running, do the following.
 - a. On a terminal session on the data server, run **su - dsrdbm01**.
 - b. Run **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** to start the application server.
9. If the Tivoli Directory Server, `ibmslapd`, is running, do the following.

Note: Do this step even if the Tivoli Directory Server was started in the previous step.

- a. Log on to a terminal session on the data server as `dsrdbm01`.
 - b. Run **idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*** where `ADMIN_PASSWORD` is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
10. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
 - a. Log on to a terminal session on the management server as `ibmadmin`.
 - b. Run the **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD** command on the management server where `WAS_ADMIN_PASSWORD` is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.


```
ADMU0508I: The Application Server "tdsServer" is STARTED
```

 If the following message is returned, the `tdsServer` needs to be started.


```
ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
```
 - c. Start the `tdsServer` by running the **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer** command. The server, `tdsServer`, will start and a message similar to the following will be displayed.


```
ADMU3000I: Server tdsServer open for e-business; process id is 26654
```
 11. Access the Tivoli Directory Server Web Administration Tool at: `http://APPLICATION_SERVER_HOST:9062/IDSWebApp/` where `APPLICATION_SERVER_HOST` is the host name of the application server.
 12. Log on with the LDAP Root Administrator Account, `cn=root`, and the appropriate password. The LDAP Server name should be `DATABASE_DIRECTORY_SERVER_HOST:389` where `DATABASE_DIRECTORY_SERVER_HOST` is the host name of the data server.
 13. Click **Server Administration > Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Account Management (Tivoli Directory Server) Test

The Account Management (Tivoli Directory Server) test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Account Management (Tivoli Directory Server) test uses the following resource:

- Tivoli Directory Server (on the data server)

Problem determination

If the **Tivoli Directory Server HTTP Test** fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere 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 file systems on the data server has not reached capacity. This can be determined using the **df -h** command.
3. Verify that the Tivoli Directory Server LDAP server is running.
 - a. Log on to a terminal session on the data server as root.
 - b. Run the **ps -ef | grep ibmslapd** command. The results will be similar to the following:

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149    0 23:17 pts/1    00:00:00 grep ibmslapd
```

This example shows that the Tivoli Directory Server daemon, **ibmslapd**, is running.
 - c. Run the **ps -ef | grep ibmdiradm** command. The results will be similar to the following:

```
root      4394 14038    0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

This example shows that the Tivoli Directory Server daemon, **ibmdiradm**, is running.
4. If the Tivoli Directory Server, **ibmslapd**, is not running, do the following.
 - a. As a **root** Linux user, run **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** to start the Directory Server
5. If the Tivoli Directory Administration Server, **ibmdiradm**, is not running, do the following.
 - a. On a terminal session on the data server, run **su - dsrdbm01**.
 - b. Run **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** to start the application server.
6. If the Tivoli Directory Server, **ibmslapd**, is running, do the following.

Note: Do this step even if the Tivoli Directory Server was started in the previous step.

- a. Log on to a terminal session on the data server as **dsrdbm01**.
 - b. Run **idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*** where **ADMIN_PASSWORD** is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
7. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
 - a. Log on to a terminal session on the management server as **ibmadmin**.
 - b. Run the **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD** command on the management server where **WAS_ADMIN_PASSWORD** is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.

```
ADMU0508I: The Application Server "tdsServer" is STARTED
```

If the following message is returned, the tdsServer needs to be started.

ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.

- c. Start the tdsServer by running the `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer` command. The server, tdsServer, will start and a message similar to the following will be displayed.

ADMU3000I: Server tdsServer open for e-business; process id is 26654

8. Access the Tivoli Directory Server Web Administration Tool at: `http://APPLICATION_SERVER_HOST:9062/IDSWebApp/` where `APPLICATION_SERVER_HOST` is the host name of the application server.
9. Log on with the LDAP Root Administrator Account, `cn=root`, and the appropriate password. The LDAP Server name should be `DATABASE_DIRECTORY_SERVER_HOST:389` where `DATABASE_DIRECTORY_SERVER_HOST` is the host name of the data server.
10. Click **Server Administration > Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Analytics (Cognos Gateway Console) Test

The Analytics (Cognos Gateway Console) test determines if Cognos, on the application server, can be accessed by the Cognos Servlet Gateway and Cognos Administration Portal URL.

Resources

The Analytics (Cognos Gateway Console) test uses the following resource:

- Cognos (on the application server system).

Problem determination

If the Analytics (Cognos Gateway Console) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following Cognos logs:
 - `/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.
2. Verify that the file systems on the application server system have not reached capacity. This can be determined using the `df -h` command.
3. Verify that Cognos Dispatcher and Cognos Gateway servers are started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `cgnsadm` (Cognos user).

- b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
- c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
- d. If message `ADMU0509I: The Application Server "CognosX_Displ" cannot be reached. It appears to be stopped.` is displayed, start CognosX_Displ using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_Displ`. Skip this step if message `ADMU0508I: The Application Server "CognosX_Displ" is STARTED.` is displayed. If you had to start CognosX_Displ, a message similar to the following will be displayed: `ADMU3000I: Server CognosX_Displ open for e-business; process id is 26654.`
- e. If message `ADMU0509I: The Application Server "CognosX_GW1" cannot be reached. It appears to be stopped.` is displayed, start CognosX_GW1 using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_GW1`. Skip this step if message `ADMU0508I: The Application Server "CognosX_GW1" is STARTED.` is displayed. If you had to start CognosX_GW1, a message similar to the following will be displayed: `ADMU3000I: Server CognosX_GW1 open for e-business; process id is 26676.`

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. CognosX_Displ
- c. CognosX_GW1

Stop servers in this order:

- a. CognosX_GW1
- b. CognosX_Displ
- c. nodeagent

The CognosX_GW1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_GW1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

The CognosX_Displ server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_Displ -wasadmin admin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.


The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that Cognos Dispatcher and Cognos Gateway servers are started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID `admin` and password. `APPLICATION_SERVER_HOST` is the host name for the application server.

- b. View the status of the CognosX-Disp1 and CognosX_GW1 servers by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. CognosX_Displ
- c. CognosX_GW1

Stop servers in this order:

- a. CognosX_GW1
- b. CognosX_Displ
- c. nodeagent

To stop the CognosX_GW1 and CognosX_Displ servers, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the Cognos Administration Portal can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://APPLICATION_SERVER_HOST:9081/ServletGateway/Servlet/Gateway`. Where the `APPLICATION_SERVER_HOST` is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (WebSphere Application Server Web Service) Test

The Application Server (WebSphere Application Server Web Service) test tests access to the WebSphere Application Server Web Service by accessing the DrpGeoSvc web service.

Resources

The Application Server (WebSphere Application Server Web Service) test uses the following resource:

- WebSphere Application Server (on the application server).

Problem determination

If the Application Server (WebSphere Application Server Web Service) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`

- b. On the application server review the following WebSphere UDDI Registry configuration logs:
 - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log
2. Verify that the file system on the application server has not reached capacity. This can be determined using the **df -h** command.
3. Verify that the cpudServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as **ibmadmin**.
 - b. In a command window, run: /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
 - c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh . Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.
 - a. If message ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped. is displayed, start cpudServer1 using the following command: /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1. Skip this step if message ADMU0508I: The Application Server "cpudServer1" is STARTED. is displayed. If you had to start cpudServer1, a message similar to the following will be displayed: ADMU3000I: Server cpudServer1 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1


Stop servers in this order:



- a. cpudServer1
- b. nodeagent

The cpudServer1 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

4. Verify that the cpudServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at http://APPLICATION_SERVER_HOST:9060/admin using the WebSphere Application Server Administrative ID **admin** and password. *APPLICATION_SERVER_HOST* is the host name for the Application Server.
 - b. View the status of the cpudServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server. The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1

Stop servers in this order:

- a. cpudServer1
- b. nodeagent

To stop the cpudServer server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the WebSphere UDDI User Console can be accessed.
 - a. On the application server, access: `https://APPLICATION_SERVER_HOST:9080/uddigui/` where `APPLICATION_SERVER_HOST` is the host name of the application server.

What to do next

Resolve any issues or errors found and retry the test.

Business Rules (WebSphere Operational Decision Manager JRules Console) Test

The Business Rules (WebSphere Operational Decision Manager JRules Console) test tests access to WebSphere Operational Decision Management JRules by accessing the Rule Execution Server Console.

Resources

The Business Rules (WebSphere Operational Decision Manager JRules Console) test uses the following resource:

- WebSphere Operational Decision Management JRules (on the application server).

Problem determination

If the Business Rules (WebSphere Operational Decision Manager JRules Console) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere Operational Decision Management configuration logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`

2. Verify that the file system on the application server has not reached capacity. This can be determined using the `df -h` command.
3. Verify that the Rule Execution Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed`, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed`. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
 - a. If message `ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped. is displayed`, start `wodmServer1` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Skip this step if message `ADMU0508I: The Application Server "wodmServer1" is STARTED. is displayed`. If you had to start `wodmServer1`, a message similar to the following will be displayed: `ADMU3000I: Server wodmServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:



- a. nodeagent
- b. wodmServer1


Stop servers in this order:

- a. wodmServer1
- b. nodeagent

The `wodmServer1` server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

The `nodeagent` is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the Rule Execution Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID `admin` and password. `APPLICATION_SERVER_HOST` is the host name for the application server.
 - b. View the status of the `wodmProfile` server by clicking **Servers > Server Types > WebSphere application servers**.
 - The  icon means the server is started. If required, select the server and click **Restart** to restart the server.
 - The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. wodmServer1

Stop servers in this order:

- a. wodmServer1
- b. nodeagent

To stop the wodmProfile server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the Rule Execution Server Console can be accessed from the application server at `http://APPLICATION_SERVER_HOST:9083/res` where `APPLICATION_SERVER_HOST` is the host name of the application server. Log on using the userid `resAdmin1`.
6. In the Rule Execution Server Console open the Diagnostics tab. Click **Run Diagnostics**. A report will be displayed with the tests run. Click **Expand All** to see the details about each test.

What to do next

Resolve any issues or errors found and retry the test.

Business Rules (WebSphere Operational Decision Manager JRules Rule) Test

The Business Rules (WebSphere Operational Decision Manager JRules Rule) tests access to the WebSphere Operational Decision Management JRules Rule Engine by calling the `cardTransactionRuleApp` business rule installed on the Rules Execution Server and verifying the output.

Resources

The Business Rules (WebSphere Operational Decision Manager JRules Rule) test uses the following resource:

- WebSphere Operational Decision Management JRules (on the application server).

Problem determination

If the Business Rules (WebSphere Operational Decision Manager JRules Rule) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere Operational Decision Management configuration logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`

2. Verify that the file system on the application server has not reached capacity. This can be determined using the `df -h` command.
3. Verify that the Rule Execution Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed`, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed`. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
 - a. If message `ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped. is displayed`, start `wodmServer1` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Skip this step if message `ADMU0508I: The Application Server "wodmServer1" is STARTED. is displayed`. If you had to start `wodmServer1`, a message similar to the following will be displayed: `ADMU3000I: Server wodmServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. wodmServer1

Stop servers in this order:

- a. wodmServer1
- b. nodeagent


The `wodmServer1` server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

The `nodeagent` is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the Rule Execution Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID `admin` and password. `APPLICATION_SERVER_HOST` is the host name for the application server.
 - b. View the status of the `wodmProfile` server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. wodmServer1

Stop servers in this order:

- a. wodmServer1
- b. nodeagent

To stop the wodmProfile server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the Rule Execution Server Console can be accessed from the application server at `http://APPLICATION_SERVER_HOST:9083/res` where `APPLICATION_SERVER_HOST` is the host name of the application server. Log on using the userid `resAdmin1`.
6. In the Rule Execution Server Console open the Diagnostics tab. Click **Run Diagnostics**. A report will be displayed with the tests run. Click **Expand All** to see the details about each test.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Domino console) Test

Collaboration (Lotus Domino console) test determines if the Domino Directory is accessible through its URL.

Resources

The Collaboration (Lotus Domino console) test uses the following resource:

- Domino Server (on the event server).

Problem determination

If the Collaboration (Lotus Domino console) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the event server review the following Lotus Domino logs:
 - `/local/notesdata/console.out`
 - `/local/notesdata/log.nsf`
 - All logs in the `/local/notesdata/IBM_TECHNICAL_SUPPORT/` directory.
2. Verify that the file systems on the event server system have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the Lotus Domino Process components are running.
 - a. Login to the Lotus Domino Directory console at `http://EVENT_SERVER_HOST:84/names.nsf` where `EVENT_SERVER_HOST` is the host name of the event server. Login using the Domino administrator username and password.

- b. If the console cannot be accessed, on the event server, run the `ps -ef | grep notes` command to determine if the Lotus Domino processes are running. The Lotus Domino processes are:
 - server
 - event
 - update
 - replica
 - router
 - adminp
 - calconn
 - sched
 - http
 - rnmgr
 - staddin
4. If some, but not all, processes are running, stop the running processes before restarting all the processes.
 - a. On the event server, login as the notes user.
 - b. Change to the `/local/notesdata` directory.
 - c. Run the `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` command to stop all running Lotus Domino processes.
 - d. Check that all processes have stopped by running the `ps -ef | grep notes` command.
 - e. If any Lotus Domino processes are still running, stop them using the `kill -9 pid` where *pid* is the process identifier of the Lotus Domino process.
5. If the Lotus Domino processes are not running, start the Lotus Domino Server components.
 - a. On the event server, login as the notes user.
 - b. Change to the `/local/notesdata` directory.
 - c. Run the `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` command to start all Lotus Domino Server components.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Sametime console) Test

Collaboration (Lotus Sametime console) test determines if the Sametime Console is accessible through its URL.

Resources

The Collaboration (Lotus Sametime console) test uses the following resource:

- Sametime Server (on the event server).

Problem determination

If the Collaboration (Lotus Sametime console) test fails, do the following to find and resolve the problem.

Procedure

1. Collect and review the Sametime Community Server configuration and log files.
 - a. Log on the event server as a *notes* user.
 - b. Change to the `/local/notesdata` directory.
 - c. Run the `sh stdiagzip.sh` command. This command will collect all pertinent log files and write them to the `/local/notesdata/` directory.

- d. Review the logs in the `/local/notesdata/` directory.
2. Verify that the file systems on the event server system have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the Sametime Process components are running.
 - a. Login to the Sametime Home page at `http://EVENT_SERVER_HOST:84/stcenter.nsf` where `EVENT_SERVER_HOST` is the host name of the event server. Login using the Domino administrator username and password.
 - b. On the Sametime Home page click **Administer the server**.
 - c. On the Server - Overview page, make sure all the Sametime services are running.
4. If some, but not all, processes are running, stop the running processes before restarting all the processes.
 - a. On the event server, login as the notes user.
 - b. Change to the `/local/notesdata` directory.
 - c. Run the `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` command to stop all running Sametime processes.
 - d. Check that all processes have stopped by running the `ps -ef | grep notes` command.
 - e. If any processes are still running, stop them by using the `kill -9 pid` where `pid` is the process identifier of the Lotus Domino process.
5. If the Sametime processes are not running, start the Lotus Sametime Server components.
 - a. On the event server, login as the notes user.
 - b. Change to the `/local/notesdata` directory.
 - c. Run the `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` command to start all Lotus Sametime Server components.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Sametime Proxy console) Test

The Collaboration (Lotus Sametime Proxy console) test determines if the Lotus Sametime Proxy Web Application can be accessed by the Lotus Sametime Proxy Web Application URL.

Resources

The Collaboration (Lotus Sametime Proxy console) test uses the following resource:

- Sametime Proxy (on the application server).

Problem determination

If the Collaboration (Lotus Sametime Proxy console) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following Sametime Proxy Server logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/logs/STProxyServer1/SystemErr.log`

2. Verify that the file systems on the application server system have not reached capacity. This can be determined using the **df -h** command.
3. Verify that the Sametime Proxy Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
 - d. If message `ADMU0509I: The Application Server "STProxyServer1" cannot be reached. It appears to be stopped.` is displayed, start `STProxyServer1` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1`. Skip this step if message `ADMU0508I: The Application Server "STProxyServer1" is STARTED.` is displayed. If you had to start `STProxyServer1`, a message similar to the following will be displayed: `ADMU3000I: Server STProxyServer1 open for e-business; process id is 26654.`

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. STProxyServer1


Stop servers in this order:

- a. STProxyServer1
- b. nodeagent


The `STProxyServer1` server is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the Sametime Proxy Server is are started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID `admin` and password. `APPLICATION_SERVER_HOST` is the host name for the application server.
 - b. View the status of the `STProxyServer1` server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. STProxyServer1

Stop servers in this order:

- a. STProxyServer1
- b. nodeagent

To stop the STProxyServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the Sametime Proxy Console can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://APPLICATION_SERVER_HOST:9085/stwebclient/popup.jsp`. Where the `APPLICATION_SERVER_HOST` is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2) Test

Database (DB2) test determines if the JDBC connection can be accessed between the web application and the data server. A JDBC type 4 connection is established and a dynamic SQL query is issued counting the number of tables present in the database.

Resources

The Database (DB2) test uses the following resources:

- UddiDataSource definition containing the connection for the UDDIDB database (on the application server).
- UDDIDB database (db2inst4 instance on the data server).

Problem determination

If the Database (DB2) test is unable to access data server, do the following to find and resolve the access problem.

Procedure

1. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`

3. Verify that the file systems on the data server system have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the databases used by the data server are started.
 - a. On the data server, run the following command from a command window as db2inst4:


```
ps -ef | grep db2 | grep db2inst4
```

DB2 processes, including the following, should be running as the db2inst4 instance user:

```
db2sysc
db2vend
db2acd
```
5. If the DB2 processes are not running, start them by running db2start from the command window as the db2inst4 user:
6. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/db2inst4/sql1lib/db2dump directory.
7. Check the db2diag.log for errors issued when starting the database used for this test.
8. Verify the connection to the DataSource web container resources using the WebSphere Application Server administrative console.
 - a. On the application server, access the WebSphere Application Server administrative console at: https://APPLICATION_SERVER_HOST:9043/ibm/console where APPLICATION_SERVER_HOST is the host name of the application server.
 - b. Click **Resources > JDBC > Data sources**.
 - c. Check the UddiDataSource data source by clicking **Test Connection** to test the connection to the data source.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - *instance*) Test

Database (DB2 Instance - *instance*) test the DB2 manager status of the DB2 instance on the data server by running the **db2status** script.

Resources

The Database (DB2 Instance - *instance*) test uses the following resource:

- The DB2 *instance* (on the data server)

Problem determination

If the Database (DB2 Instance - *instance*) test fails, do the following to find and resolve the access problem.

Procedure

1. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log

3. Verify that the file system on the data server system has not reached capacity. This can be determined using the **df -h** command.
4. Verify that the databases used by the data server are started.
 - a. On the data server, run the following command from a command window as the user *instance* where *instance* is the name of the DB2 instance indicated in the test name:


```
db2 get snapshot for dbm | grep status
```

If the database manager is started for the *instance*, the following message is displayed: Database manager status = Active.
5. If the DB2 processes are not running, start them by running **su - instance** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
6. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/instance/sql1ib/db2dump` directory.
7. Check the `db2diag.log` for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Directory (UDDI V3 and UDDI V3 HTTPS) Test

The Directory (UDDI V3 and UDDI V3 HTTPS) test determines if the WebSphere UDDI Registry can be accessed using the WebSphere UDDI Registry HTTP and HTTPS URL.

Resources

The Directory (UDDI V3 and UDDI V3 HTTPS) test uses the following resource:

- WebSphere Application Server (on the application server).

Problem determination

If the Directory (UDDI V3 and UDDI V3 HTTPS) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere UDDI Registry configuration logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log`
2. Verify that the file systems on the application server system have not reached capacity. This can be determined using the **df -h** command.
3. Verify that the `cpudServer1` server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the `nodeagent` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The`

Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

- a. If message ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped. is displayed, start cpudServer1 using the following command:
/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1. Skip this step if message ADMU0508I: The Application Server "cpudServer1" is STARTED. is displayed. If you had to start cpudServer1, a message similar to the following will be displayed: ADMU3000I: Server cpudServer1 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1

Stop servers in this order:

- a. cpudServer1
- b. nodeagent

The cpudServer1 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD where WAS_ADMIN_PWD is the WebSphere administrator password.


The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD where WAS_ADMIN_PWD is the WebSphere administrator password.

4. Verify that the cpudServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

- a. Log on to the WebSphere Application Server Administrative Console at http://APPLICATION_SERVER_HOST:9060/admin using the WebSphere Application Server Administrative ID admin and password. APPLICATION_SERVER_HOST is the host name for the Application Server.
- b. View the status of the cpudServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1

Stop servers in this order:

- a. cpudServer1
- b. nodeagent

To stop the cpudServer server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that WebSphere UDDI Registry user console can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://APPLICATION_SERVER_HOST:9080/uddigi/`. Where the `APPLICATION_SERVER_HOST` is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Internal Diagnostic (Echo REST remoted) Test

The Internal Diagnostic (Echo REST remoted) test tests access to the Remote Responder by accessing the URL. This is a diagnostic of the System Verification Check and checks the links between System Verification Check modules.

Resources

The Internal Diagnostic (Echo REST remoted) uses the following resource:

- WebSphere Application Server (on the application server).

Problem determination

If the Internal Diagnostic (Echo REST remoted) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere UDDI Registry configuration logs:
 - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log`
2. Verify that the file system on the application server has not reached capacity. This can be determined using the `df -h` command.
3. Verify that the cpudServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed`, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed`. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
 - a. If message `ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped. is displayed`, start cpudServer1 using the following command: `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startServer.sh cpudServer1`. Skip

this step if message ADMU0508I: The Application Server "cpudServer1" is STARTED. is displayed. If you had to start cpudServer1, a message similar to the following will be displayed: ADMU3000I: Server cpudServer1 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1

Stop servers in this order:

- a. cpudServer1
- b. nodeagent

The cpudServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.


The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the cpudServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

- a. Log on to the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9060/admin` using the WebSphere Application Server Administrative ID admin and password. `APPLICATION_SERVER_HOST` is the host name for the Application Server.
- b. View the status of the cpudServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. cpudServer1

Stop servers in this order:

- a. cpudServer1
- b. nodeagent

To stop the cpudServer server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that the WebSphere UDDI User Console can be accessed.

- a. On the application server, access: `https://APPLICATION_SERVER_HOST:9080/uddigui/` where `APPLICATION_SERVER_HOST` is the host name of the application server.

What to do next

Resolve any issues or errors found and retry the test.

Messaging (WebSphere Message Broker Publish/Subscribe topic) Test

The Messaging (WebSphere Message Broker Publish/Subscribe topic) test tests the WebSphere Message Broker publish and subscribe functions. The test publishes a message to the topic with JNDI name listed in the properties as `jms/IopCatWmbPub`. WebSphere Message Broker receives the message it then publishes a return message on the `IOP.CAT.PUBtopic`. The test is successful if the response message is received. The test fails if there is an error or if the response message is not received within the timeout period specified in the properties file.

Resources

The Messaging (WebSphere Message Broker Publish/Subscribe topic) test uses the following resources:

- WebSphere Portal Server (on the application server).
- WebSphere Message Queue (on the event server).
- WebSphere Message Broker (on the event server).

Problem determination

If the Messaging (WebSphere Message Broker Publish/Subscribe topic) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the event server. This can be done by sending **ping** commands with both the short and fully-qualified host name to and from each server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the event server and application server have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the WebSphere Message Queue queue manager and WebSphere Message Broker broker are running.
 - a. On the event server, log on as the WebSphere Message Queue administrator. For example, `mqm`.
 - b. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. You should see a message similar to the following:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. If a status other than Running was returned, start the WebSphere Message Queue queue manager using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
 - d. On the event server, log on as the WebSphere Message Broker administrator. For example, `mqm`.
 - e. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** You should see a message similar to the following:
`BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.`
 - f. If a status other than Running was returned, start the WebSphere Message Broker broker using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsisstart IOC_BROKER**.

5. Check the logs for errors. The logs are located on the event server in the `/var/log/messages` directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If the broker or queue managers do not appear to be started, they can also be started by starting the event server and running the startup scripts for the system.

What to do next

Resolve any issues or errors found and retry the test.

Messaging (WebSphere Message Queue Publish/Subscribe topic) Test

The Messaging (WebSphere Message Queue Publish/Subscribe topic) test tests the WebSphere Message Queue publish and subscribe functions. The test creates a topic specified in the properties. It then publishes a message to the topic and immediately tries to read the published message. The test succeeds if the sent message can be read. The test fails if there is an error or if the message cannot be read within 15 seconds (15000 milliseconds).

Resources

The Messaging (WebSphere Message Queue Publish/Subscribe topic) test uses the following resources:

- WebSphere Portal Server (on the application server).
- WebSphere Message Queue (on the event server).

Problem determination

If the Messaging (WebSphere Message Queue Publish/Subscribe topic) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and event server. This can be done by sending **ping** commands with both the short and fully-qualified host name to and from each server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the servers have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the WebSphere Message Queue queue manager is running.
 - a. On the event server, log on as the WebSphere Message Queue administrator. For example, `mqm`.
 - b. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. You should see a message similar to the following:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. If a status other than `Running` was returned, start the WebSphere Message Queue queue manager using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
5. Check the logs for errors. The logs are located on the event server in the `/var/log/messages` directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If the queue manager does not appear to be started, it can also be started by starting the event server and running the startup scripts for the system.

What to do next

Resolve any issues or errors found and retry the test.

Messaging (Message Broker install check) Test

The Messaging (Message Broker install check) test determines if the WebSphere Message Queue and Message Broker can be accessed. This is done by running the WebSphere Message Broker **mqsilist** command on the system running the WebSphere Message Broker.

Resources

The Messaging (Message Broker install check) uses the following resources:

- WebSphere Portal Server (on the application server).
- WebSphere Message Queue and Message Broker (on the event server).

Problem determination

If the Messaging (Message Broker install check) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the WebSphere Portal system (on the application server) and the WebSphere Message Broker system (on the event server). This can be done by sending **ping** commands with both the short and fully-qualified host name of the event server from the application server and vice versa. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the application server and event server systems have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the WebSphere Message Queue queue manager and WebSphere Message Broker broker are running.
 - a. On the event server, log on as the WebSphere Message Queue administrator. For example, `mqm`.
 - b. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. You should see a message similar to the following:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. If a status other than Running was returned, start the WebSphere Message Queue queue manager using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
 - d. On the event server, log on as the WebSphere Message Broker administrator. For example, `mqm`.
 - e. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist**. You should see a message similar to the following:
`BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.`
 - f. If a status other than Running was returned, start the WebSphere Message Broker broker using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.
5. Check the logs for errors. The logs are located on the event server in the `/var/log/messages` directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If the broker or queue managers do not appear to be started, they can also be started by starting the event server and running the startup scripts for the system.

What to do next

Resolve any issues or errors found and retry the test.

Messaging (WebSphere Message Broker/Queue queue) Test

The Messaging (WebSphere Message Broker/Queue queue) test tests the WebSphere Message Queue by placing a message in a queue.

Resources

The Messaging (WebSphere Message Broker/Queue queue) test uses the following resources:

- WebSphere Portal Server (on the application server).
- WebSphere Message Queue (on the event server).
- WebSphere Message Broker (on the event server).

Problem determination

If the Messaging (WebSphere Message Broker/Queue queue) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and event server. This can be done by sending **ping** commands with both the short and fully-qualified host name to and from each server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the application server and event server systems have not reached capacity. This can be determined using the **df -h** command.
4. Verify that the WebSphere Message Queue queue manager and WebSphere Message Broker broker are running.
 - a. On the event server, log on as the WebSphere Message Queue administrator. For example, `mqm`.
 - b. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq**. You should see a message similar to the following:
`QMNAME(IOC.MB.QM) STATUS(Running)`
 - c. If a status other than Running was returned, start the WebSphere Message Queue queue manager using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
 - d. On the event server, log on as the WebSphere Message Broker administrator. For example, `mqm`.
 - e. In a command window, run **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** You should see a message similar to the following:
`BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.`
 - f. If a status other than Running was returned, start the WebSphere Message Broker broker using the following command: **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.
5. Check the logs for errors. The logs are located on the event server in the `/var/log/messages` directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If the broker or queue managers do not appear to be started, they can also be started by starting the event server and running the startup scripts for the system.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Netcool Impact Console) Test

The Monitoring (Netcool® Impact Console) test determines if the Netcool Impact Console is running and accessible by the Netcool Impact Console URL.

Resources

The Monitoring (Netcool Impact Console) test uses the following resource:

- Netcool Impact Server (on the event server)

Problem determination

If the Monitoring (Netcool Impact Console) test fails, do the following to find and resolve the problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. On the event server review the following Netcool Impact logs:
 - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log
 - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
2. Verify that the file systems on the event server system have not reached capacity. This can be determined using the **df -h** command.
3. Verify that the server1 server is started.
 - a. On the event server system log on as wasadmin.
 - b. In a command window, run: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
 - c. If message ADMU0509I: The Application Server "server1" cannot be reached. It appears to be stopped. is displayed, start the server1 server, which will also start the Netcool Impact Console Server, using the following command: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1. Skip this step if message ADMU0508I: The Application Server "server1" is STARTED is displayed. If you had to start the server1 server, a message similar to the following will be displayed: ADMU3000I: Server server1 open for e-business; process id is 26654.
The server1 server is stopped by running the following command in a command window on the event server: /opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.
4. Verify that the Netcool Impact Console can be accessed from the event server: `http://EVENT_SERVER_HOST:9080/nci` where *EVENT_SERVER_HOST* is the host name of the event server.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Netcool Omnibus) Test

The Monitoring (Netcool Omnibus) test determines if Netcool Omnibus is available. This is done by running the **nco_pa_status -server NCO_PA** command.

Resources

The Monitoring (Netcool Omnibus) test uses the following resource:

- Netcool Omnibus Server (on the event server)

Problem determination

If the Monitoring (Netcool Omnibus) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the event server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the event server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Check that the Process Control server services and agent are running.
 - a. From a command window on the event server, run the `$NCHOME/omnibus/bin/nco_pa_status -server NCO_PA` command as a *netcool* Linux user.
 - b. If the services are not started or running, start the server by running the `/etc/init.d/nco start` command on the event server as a *root* Linux user.
 - c. If the process agent is not running, start the agent by running the `$NCHOME/omnibus/bin/nco_pad` command on the event server as a *netcool* Linux user.
3. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the event server review all logs beginning with NCO in the following directories:
 - `/opt/IBM/netcool/log`
 - `/opt/IBM/netcool/omnibus/log`
4. Verify that the file systems on the event server system have not reached capacity. This can be determined using the `df -h` command.
5. Verify that the Netcool Omnibus portlet can be accessed from the application server:
`http://EVENT_SERVER_HOST:9060/ibm/console` where `EVENT_SERVER_HOST` is the host name of the event server.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Tivoli Composite Application Manager Agents - server) Test

The Monitoring (Tivoli Composite Application Manager Agents - server) test tests if the Tivoli Composite Application Manager agents are running by running the `cinfo` command.

Resources

The Monitoring (Tivoli Composite Application Manager Agents - server) test uses the following resources:

- Tivoli Composite Application Manager
 - Tivoli Composite Application Manager agents (on the application server)
 - Tivoli Composite Application Manager agents (on the event server)
 - Tivoli Composite Application Manager agents (on the data server)
 - Tivoli Composite Application Manager agents (on the management server)

Problem determination

If the Monitoring (Tivoli Composite Application Manager Agents - *server*) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server, management server, event server, and data server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the management server, event server, and data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file systems on the application server, management server, event server, and data server have not reached capacity. This can be determined using the **df -h** command.
4. Repeat this step on the application server, management server, event server, and data server to verify that the Tivoli Monitoring components are running.
 - a. Log on to a terminal session on the server as root.
 - b. Run the `/opt/IBM/ITM/bin/cinfo -r` command. Results similar to the following will be displayed. The agents will differ on the different servers. The agents should have a status of running.

```
***** Sun May 13 02:13:26 EDT 2012 *****
User: root Groups: root bin daemon sys adm disk wheel idsldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
*****
Host  Prod  PID  Owner  Start  ID  ..Status
baapp2 lz    31042 root   May09  None  ...running
baapp2 ht    18755 root   May09  None  ...running
baapp2 yn    4190 root   02:11  None  ...running
```

- c. Start any Tivoli Composite Application Manager agents that are not running.
 - 1) Log on to a terminal session on the server as root.
 - 2) Run the `/opt/IBM/ITM/bin/itmcmd agent start PRODUCT_CODE` where `PRODUCT_CODE` is the PID value for an agent found in the results of the `/opt/IBM/ITM/bin/cinfo -o` command.
5. Review the log files for exceptions.
 - a. On the management server review the following Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server logs:
 - Tivoli Enterprise Monitoring Server: `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log`
 - Tivoli Enterprise Portal Server: `/opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log`where `PRODUCT_CODE` is the PID return by the `/opt/IBM/ITM/bin/cinfo -o` command.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Tivoli Enterprise Monitoring Server) Test

The Monitoring (Tivoli Enterprise Monitoring Server) test determines if the Tivoli Enterprise Monitoring Server running on the management server is available. A query requesting the component status is sent to the Tivoli Monitoring Web Services SOAP server. The query includes an invalid user ID and password for the system. The response should indicate that an invalid ID or password was used. The error indicates that the Tivoli Enterprise Monitoring Server is operating correctly.

Resources

The Monitoring (Tivoli Enterprise Monitoring Server) test uses the following resources:

- Tivoli Enterprise Monitoring System (on the management server)
 - Tivoli Monitoring Web Services SOAP Server
 - Tivoli Enterprise Portal Server
 - Tivoli Enterprise Portal Server DB2 database

Problem determination

If the Monitoring (Tivoli Enterprise Monitoring Server) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity between the application server and the management server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the management server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the management server review the following management server logs:
 - 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:
 - 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`
3. Verify that the file systems on the management server has not reached capacity. This can be determined using the **df -h** command.
4. Verify that the Tivoli Monitoring components are running on the management server.
 - a. Log on to a terminal session on the management server as `root`.
 - b. Run the `/opt/IBM/ITM/bin/cinfo -r` command.
5. Verify that the Tivoli component databases are operational.
 - a. Log on to a terminal session on the management server as `db2inst1`.
 - b. Run the `ps -ef | grep db2inst1` command.
 - c. Verify that the DB2 processes are running. These include `db2sysc`, `db2vend`, and `db2acd`.
 - d. If the DB2 processes are not running, run the `$> db2start` command.
 - e. Check the DB2 logs on the data server for any database errors related starting databases used by Tivoli components. The log files can be found in the `/datahome/db2inst1/sql1lib/db2dump` directory on the data server.
6. In the results, verify that the Tivoli Enterprise Monitoring Server is running by looking for an entry for `ms`. If the entry is not listed, the Tivoli Enterprise Monitoring Server is not running.
7. If the Tivoli Enterprise Monitoring Server is not running, start the server.
 - a. Log on to a terminal session on the management server as `root`.
 - b. Run the `/opt/IBM/ITM/bin/itmcmd server start HUB_MMOS` command.
8. In the results from step 4, verify that the Tivoli Enterprise Portal Server is running by looking for an entry for `cq`. If the entry is not listed, the Tivoli Enterprise Portal Server is not running.

9. If the Tivoli Enterprise Portal Server is not running, start the server.
 - a. Log on to a terminal session on the management server as root.
 - b. Run the `/opt/IBM/ITM/bin/itmcmd agent start cq` command.
10. In the results from step 4 on page 232, verify that other valid subcomponents are running.

Table 79. Tivoli Monitoring components

| Component | Description |
|-----------|---|
| kf | Eclipse Help Server |
| cq | Tivoli Enterprise Portal Server |
| lz | Monitoring Agent for Linux OS |
| ms | Tivoli Enterprise Monitoring Server |
| yn | IBM Tivoli Composite Application Manager Agent for WebSphere Applications |

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (WebSphere Business Monitor Business Space Console) Test

The Monitoring (WebSphere Business Monitor Business Space Console) test determines if WebSphere Business Monitor Business Space can be accessed using the WebSphere Business Monitor Business Space HTTP URL.

Resources

The Monitoring (WebSphere Business Monitor Business Space Console) test uses the following resource:

- WebSphere Application Server (on the application server).

Problem determination

If the Monitoring (WebSphere Business Monitor Business Space Console) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere Business 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`
2. Verify that the file systems on the application server system have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the WebSphere Business Monitor server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.

- c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh. Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.
- a. If message ADMU0509I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped. is displayed, start WBM_DE.AppTarget.WBMNode1.0 using the following command: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0. Skip this step if message ADMU0508I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" is STARTED. is displayed. If you had to start WBM_DE.AppTarget.WBMNode1.0, a message similar to the following will be displayed: ADMU3000I: Server WBM_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:




- a. nodeagent
- b. WBM_DE.AppTarget.WBMNode1.0

Stop servers in this order:

- a. WBM_DE.AppTarget.WBMNode1.0
- b. nodeagent

The WBM_DE.AppTarget.WBMNode1.0 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS_ADMIN_PWD where WAS_ADMIN_PWD is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD where WAS_ADMIN_PWD is the WebSphere administrator password.

4. Verify that the WebSphere Business Monitor server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at http://APPLICATION_SERVER_HOST:9060/admin using the WebSphere Application Server Administrative ID admin and password. APPLICATION_SERVER_HOST is the host name for the application server.
 - b. View the status of the WBM_DE.AppTarget.WBMNode1.0 server by clicking **Servers > Server Types > WebSphere application servers**.
 - The  icon means the server is started. If required, select the server and click **Restart** to restart the server.
 - The  icon means the server is stopped. Select the server and click **Start** to start the server.
 - The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. WBM_DE.AppTarget.WBMNode1.0

Stop servers in this order:

- a. WBM_DE.AppTarget.WBMNode1.0
- b. nodeagent

To stop the WBM_DE.AppTarget.WBMNode1.0 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that WebSphere Business Monitor Business Space can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://APPLICATION_SERVER_HOST:9084/BusinessSpace`. Where the `APPLICATION_SERVER_HOST` is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (WebSphere Business Monitor Mobile Device Console) Test

The Monitoring (WebSphere Business Monitor Mobile Device Console) test determines if WebSphere Business Monitor Mobile can be accessed using the WebSphere Business Monitor Mobile HTTP URL.

Resources

The Monitoring (WebSphere Business Monitor Mobile Device Console) test uses the following resource:

- WebSphere Application Server (on the application server).

Problem determination

If the Monitoring (WebSphere Business Monitor Mobile Device Console) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the application server review the following WebSphere Business 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`
2. Verify that the file systems on the application server system have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the WebSphere Business Monitor server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the application server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Skip this step if message `ADMU0508I: The`

Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

- a. If message ADMU0509I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped. is displayed, start WBM_DE.AppTarget.WBMNode1.0 using the following command: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0. Skip this step if message ADMU0508I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" is STARTED. is displayed. If you had to start WBM_DE.AppTarget.WBMNode1.0, a message similar to the following will be displayed: ADMU3000I: Server WBM_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:




- a. nodeagent
- b. WBM_DE.AppTarget.WBMNode1.0

Stop servers in this order:

- a. WBM_DE.AppTarget.WBMNode1.0
- b. nodeagent

The WBM_DE.AppTarget.WBMNode1.0 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password *WAS_ADMIN_PWD* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

4. Verify that the WebSphere Business Monitor server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
 - a. Log on to the WebSphere Application Server Administrative Console at http://APPLICATION_SERVER_HOST:9060/admin using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
 - b. View the status of the WBM_DE.AppTarget.WBMNode1.0 server by clicking **Servers > Server Types > WebSphere application servers**.
 - The  icon means the server is started. If required, select the server and click **Restart** to restart the server.
 - The  icon means the server is stopped. Select the server and click **Start** to start the server.
 - The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. WBM_DE.AppTarget.WBMNode1.0

Stop servers in this order:

- a. WBM_DE.AppTarget.WBMNode1.0

b. nodeagent

To stop the WBM_DE.AppTarget.WBMNode1.0 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that WebSphere Business Monitor Mobile can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://APPLICATION_SERVER_HOST:9084/mobile`. Where the `APPLICATION_SERVER_HOST` is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Policy (Tivoli Service Request Manager Maximo Console) Test

The Policy (Tivoli Service Request Manager Maximo Console) test determines if the Tivoli Service Request Manager Maximo can be accessed using the Tivoli Service Request Manager Maximo Start Center page.

Resources

The Policy (Tivoli Service Request Manager Maximo Console) test uses the following resource:

- Tivoli Service Request Manager Maximo (on the event server).

Problem determination

If the Policy (Tivoli Service Request Manager Maximo Console) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
 - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
 - b. On the event server review the following Tivoli Service Request Manager logs:
 - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log`
 - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log`
2. Verify that the file systems on the event server and application server systems have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the Tivoli Service Request Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
 - a. On the event server system log on as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh`. Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
 - a. If message `ADMU0509I: The Application Server "MXServer1" cannot be reached. It appears to be stopped.` is displayed, start `MXServer1` using the following command: `/opt/IBM/WebSphere/`

AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1. Skip this step if message ADMU0508I: The Application Server "MXServer1" is STARTED. is displayed. If you had to start MXServer1, a message similar to the following will be displayed: ADMU3000I: Server MXServer1 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. MXServer1

Stop servers in this order:

- a. MXServer1
- b. nodeagent

The MXServer1 server is stopped by running the following command in a command window on the event server: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.


The nodeagent is stopped by running the following command in a command window on the event server: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the Tivoli Service Request Manager server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

- a. Log on to the WebSphere Application Server Administrative Console at `http://EVENT_SERVER_HOST:9061/admin` using the WebSphere Application Server Administrative ID `admin` and password. `EVENT_SERVER_HOST` is the host name for the event server.
- b. View the status of the MXServer1 server by clicking **Servers > Server Types > WebSphere application servers**.

The  icon means the server is started. If required, select the server and click **Restart** to restart the server.

The  icon means the server is stopped. Select the server and click **Start** to start the server.

The  icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

- a. nodeagent
- b. MXServer1

Stop servers in this order:

- a. MXServer1
- b. nodeagent

To stop the MXServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the event server: `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

5. Verify that Tivoli Service Request Manager Maximo Start Center page can be accessed from the WebSphere Portal system, on the event server, using following URL: `http://EVENT_SERVER_HOST:31015/maximo/ui/login`. Where the `EVENT_SERVER_HOST` is host name for the event server. The user ID is `maxadmin`.

What to do next

Resolve any issues or errors found and retry the test.

Security (Tivoli Access Manager) Test

The Security (Tivoli Access Manager) test determines if Tivoli Access Manager is running by sending a `pd_start` command from the management server and verifying the results.

Resources

The Security (Tivoli Access Manager) test uses the following resource:

- Tivoli Access Manager including the Policy and Authorization Servers (on the management server)

Problem determination

If the Security (Tivoli Access Manager) test fails, do the following to find and resolve the problem.

About this task

In the following steps, `pdmgrd` is the Tivoli Access Manager Authorization Server, `pdmgrproxyd` is the Policy Proxy Server, and `webseald-default` is the Tivoli Access Manager WebSEAL Server.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the management server review the following Tivoli Access Manager logs:
 - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
 - `/var/PolicyDirector/log/msg__pdacl_d_utf8.log`
 - b. On the application server review the following Tivoli Access Manager logs:
 - `/var/pdweb/log/msg_*.log` where `*` is any value.
 - `/var/pdweb/log/config_data_*.log` where `*` is any value.
2. Verify that the file systems on the management server and application server systems have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the required Tivoli Access Manager components are running.
 - a. Log on to a terminal session on the management server as `root`.
 - b. Run the `pd_start status` command. The results will be similar to the following:

Tivoli Access Manager servers

| Server | Enabled | Running |
|-------------|---------|---------|
| pdmgrd | yes | yes |
| pdacl_d | yes | yes |
| pdmgrproxyd | no | no |

- c. If the `pdmgrd` or `pdacl_d` servers are not running, start them by running the `pd_start start` command.

Note: Only the `pdmgrd` and `pdacl_d` servers are enable on the management server. Both are started with the `pd_start start` command and both can be stopped with the `pd_start stop` command.
4. Verify that the required Tivoli Access Manager WebSEAL components are running.
 - a. Log on to a terminal session on the application server as `root`.

- b. Run the **pd_start status** command. The results will be similar to the following:

Tivoli Access Manager servers

| Server | Enabled | Running |
|------------------|---------|---------|
| pdmgrd | no | no |
| pdacld | no | no |
| pdmgrproxyd | no | no |
| webseald-default | yes | yes |

- c. If the webseald-default server is not running, start it by running the **pd_start start** command.

Note: Only the webseald-default server is enabled on the application server. It is started with the **pd_start start** command and can be stopped with the **pd_start stop** command.

What to do next

Resolve any issues or errors found and retry the test.

Security (Tivoli Access Manager Web Portal Manager) Test

The Security (Tivoli Access Manager Web Portal Manager) test determines if the Tivoli Access Manager Web Portal application can be accessed by the Tivoli Access Manager Web Portal application URL.

Resources

The Security (Tivoli Access Manager Web Portal Manager) test uses the following resource:

- Tivoli Access Manager - Web Portal Manager (on the management server).

Problem determination

If the Security (Tivoli Access Manager Web Portal Manager) test fails, do the following to find and resolve the access problem.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the application server review the following WebSphere Portal logs:
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
 - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
 - b. On the management server review the following Tivoli Access Manager - WebSphere Portal Manager logs:
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
 - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
2. Verify that the file systems on the management server system have not reached capacity. This can be determined using the **df -h** command.
3. Verify that the Tivoli Access Manager - Web Portal Manager is started.
 - a. On the management server log in as `ibmadmin`.
 - b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere Application Server administrator password.
 - c. If message `ADMU0509I: The Application Server "dmgr" cannot be reached. It appears to be stopped.` is displayed, start `dmgr` using the following command: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh`. Skip this step if message `ADMU0508I: The Application Server "dmgr" is STARTED.` is displayed. If you had to start `dmgr`, a message similar to the following will be displayed: `ADMU3000I: Server dmgr open for e-business; process id is 26654.`

The WebSphere Application Server Deployment Manager, including the Tivoli Access Manager - Web Portal Manager, is stopped by running the following command in a command window on the management server: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password WAS_ADMIN_PWD` where `WAS_ADMIN_PWD` is the WebSphere administrator password.

4. Verify that the Tivoli Access Manager - Web Portal Manager can be accessed from the WebSphere Portal system,
 - a. On the management server, access the following URL: `http://MANAGEMENT_SERVER_HOST9060/admin`. Where `MANAGEMENT_SERVER_HOST` is the host name for the management server.
 - b. Click **Tivoli Access Manager > Web Portal Manager > Users > Search Users**.
 - c. Log on using as user `sec_master`.

What to do next

Resolve any issues or errors found and retry the test.

Security (WebSEAL Console) Test

The Security (WebSEAL Console) test determines if Tivoli Access Manager and Tivoli Access Manager WebSEAL are running with the required resources by accessing the WebSEAL HTTP URL on Port 80 and it checking the returned page for the string "Intelligent Operations Center".

Resources

The Security (WebSEAL Console) test uses the following resources:

- Tivoli Access Manager including the Policy and Authorization Servers (on the management server)
- Tivoli Access Manager WebSEAL (on the application server)

Problem determination

If the Security (WebSEAL Console) test fails, do the following to find and resolve the problem.

About this task

In the following steps, `pdmgrd` is the Tivoli Access Manager Authorization Server, `pdmgrproxyd` is the Policy Proxy Server, and `webseald-default` is the Tivoli Access Manager WebSEAL Server.

Procedure

1. Review the log files for runtime exceptions.
 - a. On the management server review the following Tivoli Access Manager logs:
 - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
 - `/var/PolicyDirector/log/msg__pdacld_utf8.log`
 - b. On the application server review the following Tivoli Access Manager logs:
 - `/var/pdweb/log/msg__*.log` where `*` is any value.
 - `/var/pdweb/log/config_data__*.log` where `*` is any value.
2. Verify that the file systems on the management server and application server systems have not reached capacity. This can be determined using the `df -h` command.
3. Verify that the required Tivoli Access Manager components are running.
 - a. Log on to a terminal session on the management server as `root`.
 - b. Run the `pd_start status` command. The results will be similar to the following:

```
Tivoli Access Manager servers
Server      Enabled   Running
```

```

-----
pdmgrd      yes      yes
pdacld      yes      yes
pdmgrproxyd no       no

```

- c. If the pdmgrd or pdacld servers are not running, start them by running the **pd_start start** command.

Note: Only the pdmgrd and pdacld servers are enable on the management server. Both are started with the **pd_start start** command and both can be stopped with the **pd_start stop** command.

4. Verify that the required Tivoli Access Manager WebSEAL components are running.
 - a. Log on to a terminal session on the application server as root.
 - b. Run the **pd_start status** command. The results will be similar to the following:

Tivoli Access Manager servers

```

Server      Enabled  Running
-----
pdmgrd      no       no
pdacld      no       no
pdmgrproxyd no       no
webseald-default yes      yes

```

- c. If the webseald-default server is not running, start it by running the **pd_start start** command.

Note: Only the webseald-default server is enabled on the application server. It is started with the **pd_start start** command and can be stopped with the **pd_start stop** command.

What to do next

Resolve any issues or errors found and retry the test.

Web Server (IBM HTTP Server Console) Test

The Web Server (IBM HTTP Server Console) test tests access to the IBM HTTP Server by accessing the IBM HTTP Server URL.

Resources

The Web Server (IBM HTTP Server Console) uses the following resource:

- IBM HTTP Server (on the application server).

Problem determination

If the Web Server (IBM HTTP Server Console) test fails, do the following to find and resolve the problem.

Procedure

1. Check that there is network connectivity to the application server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
2. Review the log files for runtime exceptions.
 - a. On the application server review the following IBM HTTP logs:
 - /opt/IBM/HTTPServer/logs/error_log
 - /opt/IBM/HTTPServer/logs/access_log
3. Verify that the file system on the application server has not reached capacity. This can be determined using the **df -h** command.
4. Verify that the IBM HTTP Server default page can be accessed from the WebSphere Portal system.

- a. On the application server, access: `https://APPLICATION_SERVER_HOST:82/` where `APPLICATION_SERVER_HOST` is the host name of the application server.
- b. If the default page cannot be accessed, run the `ps -ef | grep HTTPServer` command to determine if the IBM HTTP Server processes are running. The IBM HTTP Server processes begin with `/opt/IBM/HTTPServer/bin/httpd`. There will be seven processes.
- c. If some, but not all, processes are running, stop the running processes before restarting all the processes.
 - 1) On the application server, login as root.
 - 2) Change to the `/opt/IBM/HTTPServer/bin` directory.
 - 3) Run the following commands to stop all running IBM HTTP processes:


```
./apachectl stop
./adminctl stop
```
 - 4) Verify that all processes have stopped by running the `ps -ef | grep HTTPServer` command.
 - 5) If any IBM HTTP Server processes are still running, stop them by using the `kill -9 pid` where `pid` is the process identifier of the IBM HTTP Server process.
- d. If the HTTP Server processes are not running, start the IBM HTTP Server components.
 - 1) On the application server, log on as root.
 - 2) Change to the `/opt/IBM/HTTPServer/bin` directory.
 - 3) Run the following commands to start all running IBM HTTP processes:


```
./adminctl start
./apachectl start
```
 - 4) Verify that all processes have started by running the `ps -ef | grep HTTPServer` command.

What to do next

Resolve any issues or errors found and retry the test.

Intelligent Operations Center Event Flow Test

The Intelligent Operations Center Event Flow test verifies if the critical components related to IBM Intelligent Operations Center event processes are working as expected. This is done by simulating external events and determining if the results are as expected.

Resources

The Intelligent Operations Center Event Flow test uses the following resource:

- IBM WebSphere Message Broker (on the application server).
- IBM WebSphere Message Queue (on the application server).
- IBM Netcool/OMNIBus (on the event server).
- IBM Netcool/Impact (on the event server).
- IBM DB2 (on the data server).

Problem determination

If the Intelligent Operations 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 management server, run `/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password` where `password` is the IBM 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/IOCControl.sh start component_ID password` 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/IOCControl.sh help`.
2. Review the Netcool/OMNIBus log (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) on the event server for any errors.
3. If necessary, 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/probes/linuxx86/ioc_xml.props &
```

What to do next

Resolve any issues or errors found and retry the test.

Intelligent Operations Center Notification Flow Test

The Intelligent Operations Center Notification Flow test verifies if the critical components related to IBM Intelligent Operations Center notification processes are working as expected. This is done by simulating external notifications and determining if the results are as expected.

Resources

The Intelligent Operations Center Notification Flow test uses the following resource:

- IBM WebSphere Message Queue (on the application server).
- IBM Netcool/OMNIBus (on the event server).
- IBM Netcool/Impact (on the event server).
- IBM DB2 (on the data server).

Problem determination

If the Intelligent Operations Center Notification 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 management server, run `/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all password` where *password* is the IBM 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/IOCControl.sh start component_ID password` 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/IOCControl.sh help`.
2. Review the Netcool/OMNIBus log (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) on the event server for any errors.
3. If necessary, 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/probes/linuxx86/ioc_xml.props &
```

What to do next

Resolve any issues or errors found and retry the test.

Chapter 7. Maintaining the solution

Perform the tasks described in this section to keep your solution running smoothly.

Backing up data

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 good practice to develop a backup procedure for the items you have added, for example:

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

Also consider data that you have accumulated, for example:

- Common Access Protocol (CAP) database data
- IBM WebSphere Business Monitor database data
- Lightweight Directory Access Protocol (LDAP) user registry data
- Geographical Information System (GIS) data

Adopt a naming convention to make it easier to identify the extensions you have added. In general, track the data that you have created or accumulated since you installed the original solution. Implement procedures for backing up the data, so that when you upgrade the solution, you do not lose valuable data.

Backing up databases

The following table lists the databases that it is recommended you back up in IBM Intelligent Operations Center.

Table 80. IBM Intelligent Operations Center databases

| Service or component | Database instance | Database names | Server |
|--|-------------------|--|-------------|
| Intelligent Operations Center database | db2inst1 | <ul style="list-style-type: none">• IOCDB | Data server |
| Portal | db2inst2 | <ul style="list-style-type: none">• CUSTDB• FDBKDB• LKMDDDB• JCRDB• COMMDB• RELDB | Data server |
| Business intelligence | db2inst3 | <ul style="list-style-type: none">• CXLOGDB• CXCONTDB | Data server |

Table 80. IBM Intelligent Operations Center databases (continued)

| Service or component | Database instance | Database names | Server |
|---|-------------------|---|-------------|
| Business rule and business activity monitor | db2inst4 | <ul style="list-style-type: none"> • UDDIDB • WODMDCDB • MONITOR • WBMDB • RESDB | Data server |
| Semantic model | db2inst5 | <ul style="list-style-type: none"> • JTS • IIC | Data server |
| Service request management | db2inst6 | <ul style="list-style-type: none"> • MAXIMO | Data server |
| Identity management | db2inst7 | <ul style="list-style-type: none"> • TIMDB | Data server |
| Applications | db2inst8 | <ul style="list-style-type: none"> • LDAPDB • LDAPDB2B | Data server |

Creating virtual infrastructure snapshots

Most virtual infrastructures have a snapshot feature that preserves the state and data of your virtual environment at a specific point in time. It is highly recommended that you take a snapshot of your environment before performing 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 on how to properly back up your virtual environment by carefully reading the instructions in the administration guide provided by the virtual infrastructure vendor.

Related tasks:

“Back up before customizing KPIs” on page 164

Back up and restore KPIs which have been created or modified with IBM WebSphere Business Monitor, or with the Key Performance Indicators portlet.

Related information:



IBM Smarter Cities Software Solutions Redbooks

Tuning performance

The following sections describe how to tune the application server and WebSphere Application Server.

Related information:



IBM Websphere Portal V 7.0 Performance Tuning Guide



IBM Websphere Application Server, Network Deployment, Version 7.0 Information Center

Tuning the application server

About this task

Use the following guidelines, which are based on the results of performance tests, to set the Java virtual machine heap size.

Procedure

1. Set the minimum and maximum heap sizes to the same values.
2. Set the heap size to a value that is compatible with the physical memory and that is above 2 GB.

What to do next

For more information, see the related link at the end of the topic.

Tuning WebSphere Application Server

For information about tuning the performance of WebSphere Application Server Version 7, see the related link at the end of the topic.

Managing log files

IBM Intelligent Operations Center stores log files in several different locations. To prevent system performance issues, periodically archive log files and remove the original log files.

If you do not manage log files and the number of log files increases indefinitely, the log files can eventually fill up a file system partition. Filling up a file system partition might have negative consequences and potentially cause the system to stop.

For information about the log files that are available in IBM Intelligent Operations Center, see the link at the end of the topic.

Related concepts:

“Troubleshooting the components” on page 284

You can use the System Verification Check tool to troubleshoot components in the IBM Intelligent Operations Center.

Updating the LTPA token for single sign-on

IBM Intelligent Operations Center uses a Lightweight Third-Party Authentication (LTPA) token to enable single sign-on across many services. The token and keys generated during installation do not expire. It is a good security practice to periodically regenerate the LTPA token and update the services using it.

Before you begin

The IBM Intelligent Operations Center product must be installed and all services started before updating the LTPA token.

This procedure requires that all services are stopped and started, so the update should not be done while the system is in production. Any users logged into the system will experience a service disruption and can lose data.

Procedure

Generate a new LTPA token for the application server

1. On the application server open a web browser and go to `http://application_host:9060/ibm/console` where `application_host` is the host name of the application server.
2. Log on as the `webwasadmin` user with the password specified in the topology properties file `WAS.ADMIN.ACCOUNT.PWD` parameter.
3. Click **Security > Global Security > Authentication mechanisms and expiration > LTPA > Generate Keys**.

4. Enter a password twice for the new LTPA token. The password is used to encrypt the LTPA token. This password will be used when importing the LTPA token. Record the password as the `WAS.LTPA.PWD` parameter in the topology properties file.
5. Enter the path and filename where the LTPA token will be saved, for example, `/tmp/newapp.ltpa`. If you specify a different path or file name, substitute your path and filename for `/tmp/newapp.ltpa` in the rest of these steps.
6. Click **Export Keys**. The new LTPA token is saved as `/tmp/newapp.ltpa`.
7. Click **Messages > Save**. Updates will be saved. Ignore any warnings about the single sign-on domain not being defined.

Copy the new LTPA token to the event server.

8. On the application server, log on as the root user and open a terminal window.
9. Run the `cp /tmp/newapp.ltpa /tmp/stproxy.ltpa` command. This replaces the file that was created when IBM Intelligent Operations Center was installed.
10. Run the `scp /tmp/newapp.ltpa root@event_host :/tmp/newapp.ltpa` command where `event_host` is the host name of the event server. When prompted, enter the root password for the event server. The LTPA token is copied to the event server.

Import the new LTPA token

11. On the event server open a web browser and go to `http://event_host:9061/ibm/console` where `event_host` is the fully-qualified host name of the event server.
12. Log on as the `webwasadmin` user with the password specified in the topology properties file `TSRM.WAS.ADMIN.PWD` parameter.
13. Click **Security > Secure administration, applications, and infrastructure > Authentication mechanisms and expiration**.
14. Enter the password for the LTPA token and `/tmp/newapp.ltpa` for the file name.
15. Click **Import Keys**.
16. Click **Messages > Save**. Updates will be saved.

Generate a new LTPA token for the event server.

17. Click **Authentication mechanisms and expiration > Generate Keys**.
18. Enter a password twice for the new LTPA token. This password will be used when importing the LTPA token.
19. Enter the path and filename where the LTPA token will be saved, for example, `/tmp/newevent.ltpa`. If you specify a different path or file name, substitute your path and filename for `/tmp/newevent.ltpa` in the rest of these steps.
20. Click **Export Keys**. The new LTPA token is saved as `/tmp/newevent.ltpa`.

Copy the new event server LTPA token to the application server.

21. On the application server, log on as the root user and open a terminal window.
22. Run the `scp /tmp/newevent.ltpa root@event_host :/tmp/newevent.ltpa` command where `event_host` is the host name of the event server. When prompted, enter the root password for the event server. The LTPA token is copied to the event server.

Update the security service with the new LTPA token.

23. On the application server log on as the root user and open a terminal window.
24. Run the `cp /tmp/newapp.ltpa /opt/pdweb/etc/` command.
25. Run the `cp /tmp/newevent.ltpa /opt/pdweb/etc/` command.
26. Create a command file named `/tmp/pd.com` containing the following commands:

```
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task default-webseald-application_host create -t tcp -h application_host -p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task default-webseald-application_host create -t tcp -h event_host -p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsrm
```

Where:

application_host
is the fully-qualified host name of the application server.

event_host
is the fully-qualified host name of the event server.

appLTPApw
is the password specified when creating the LTPA token for the application server.

eventLTPApw
is the password specified when creating the LTPA token for the event server.

27. Run the `/opt/PolicyDirector/bin/pdadmin -a sec_master -p password / tmp/pd.com` command where *password* is the password defined in the topology properties file TAM.WEBSEAL.ADMIN.PWD parameter.

Update single sign-on for the collaboration service.

28. Follow the steps in “Configuring single sign-on for collaboration services” on page 50 to update single sign-on for the collaboration service.

Stop and restart all services.

29. Using the Platform Control Tool stop all services.
30. Using the Platform Control Tool start all services. LTPA tokens will be propagated to all services.

Maintenance tips

Additional tips for maintaining the solution are documented in the form of individual technotes in the IBM Support Portal.

The following link launches a customized query of the live Support knowledge base for all versions of IBM Intelligent Operations Center: [View all maintenance tips for IBM Intelligent Operations Center.](#)

Chapter 8. Using the solution interface

The IBM Intelligent Operations Center is a web-based solution using portal technology. You can access the solution with any of the supported web browsers.

For information about supported web browsers, see the link at the end of the topic.

Related information:

 [Supported browsers for the IBM Intelligent Operations Center](#)

Logging on

Log on to access the IBM Intelligent Operations Center user interface.

Before you begin

Contact your local administrator to obtain your user ID and password. Your administrator is responsible for ensuring that you have the security access level appropriate to your role in your organization. Your administrator will also supply you with the web address URL for accessing the solution portal.

About this task

Use the following procedure to start a new browser session and access the IBM Intelligent Operations Center. You can also access the solution from other IBM Smarter Cities Software Solutions installed in your environment. From the main navigation bar at the top of the portal, select the **Intelligent Operations Center**.

Procedure

1. Enter the URL into the address field of the browser.

Note: The fully qualified domain name is required in the URL, for example, `http://application_server_hostname/wpsv70/wps/myportal`. If you use the IP address instead of the registered fully qualified domain, some portlets do not display correctly.

2. On the login page, enter your user ID and password.
3. Click **Sign In**.

Results

Only the pages, features, and data that you have permission to access are displayed. Contact your administrator if you require more access.

Related tasks:

“Logging off”

Log off to exit the IBM Intelligent Operations Center user interface and end the server session. By default, the **Log Out** link is located in the upper right corner of the IBM Intelligent Operations Center.

Logging off

Log off to exit the IBM Intelligent Operations Center user interface and end the server session. By default, the **Log Out** link is located in the upper right corner of the IBM Intelligent Operations Center.

Related tasks:

“Logging on” on page 251

Log on to access the IBM Intelligent Operations Center user interface.

Viewing or editing your user profile

You can view or change the information in your user profile for the IBM Intelligent Operations Center.

About this task

Your profile contains information previously entered by you or your administrator. You can update your profile by editing the information in attribute fields. For example, you can change your existing password to a new one.

Table 81. IBM Intelligent Operations Center user profile attributes

| Attribute | Description | User can edit? |
|------------|---|----------------|
| User ID* | An ID is assigned to each new user by the administrator for identification purposes. | No |
| Password* | A password is assigned by the administrator for security. The password must be unique and 5 - 60 characters in length. Valid passwords must contain only the characters a-z, A-Z, period ".", dash "-", and underscore "_". | Yes |
| First Name | A first name, or given name, can be entered by the administrator or the user. | Yes |
| Last Name* | A last name, or family name, is entered by the administrator. | Yes |
| Email | An email address can be entered by the administrator or the user. | Yes |

Note: Attributes marked with an asterisk are required for the successful creation of a new user. Attributes not marked with an asterisk are optional.

Procedure

1. On the right of the top navigation bar, select **Edit My Profile**. The attributes for your profile are displayed.
2. To change your password:
 - a. Enter your current password (password text is not displayed).
 - b. In the **New Password** field and **Confirm Password** fields, enter your new password.
3. Enter or edit information in any of the remaining fields.
4. To submit your changes, click **OK**.

Results

Your user profile is updated with any changes.

Using pages

A page consists of one or more complementary portlets. Using the IBM Intelligent Operations Center, you can interact with the portlets on a page to access the information that you need and respond to events as required.

The IBM Intelligent Operations Center provides six different sample page views.

Administrator

If you have administrator access, in the page view, you can access the portal service for managing pages. You can edit a page or create a new page. Click the right side of the page name tab and select an option from the page menu. For more information, see the link at the end of the topic.

Related tasks:

“Creating or customizing a page” on page 138

You can create new pages to be included in the IBM Intelligent Operations Center, and specify which portlets to display on those pages. You can customize the appearance and layout of the portlets included on each page.

Supervisor: Status view

Use the Supervisor: Status view to obtain a consolidated view of key performance indicators (KPIs) and key events. The Supervisor: Status view enables users with cross-organization responsibility to monitor, manage, and respond to status changes in relation to the key areas of organizational performance and well-being.

The Supervisor: Status view is an interactive web page. The page contains the portlets listed in Table 82. The portlets are independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the executive level.

Table 82. Supervisor: Status view portlets

| Portlet | Description |
|--|---|
| “Status” on page 274 | The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary. |
| “Key Performance Indicator Drill Down” on page 260 | To focus on a specific KPI category in the Key Performance Indicator Drill Down portlet, click the category in the Status portlet. This category is then displayed on its own in the Key Performance Indicator Drill Down portlet. You can use the list to inspect the underlying KPIs until you reach details of the KPI that caused the status change. |
| “Notifications” on page 271 | The Notifications portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts. For example, when a KPI changes status from yellow to red, an alert is sent to the Notifications portlet. |
| “My Activities” on page 269 | A user who is logged on can view the activities that are assigned to them in the My Activities portlet. In the My Activities portlet, the activities are grouped by their parent standard operating procedures. Each standard operating procedure corresponds to an individual event. |
| “Contacts” on page 257 | The Contacts portlet can display a list of your contacts that are organized by category. You can organize contacts in categories that are based on the people you need to communicate with. For example, you can have a category for general work contacts and another category for project work contacts. With the Contacts portlet, you can communicate with people and modify your online status, contacts, or groups. |

Supervisor: Operations view

Use the Supervisor: Operations view to obtain an overview of events as they happen. The Supervisor: Operations view is intended for supervisors and managers monitoring current events and planning future events.

The Supervisor: Operations view is an interactive web page. The page contains the portlets listed in Table 83. The portlets are independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the managerial level.

Table 83. Supervisor: Operations view portlets

| Portlet | Description |
|-----------------------------|--|
| "Map" on page 264 | <p>A map of the geographical region with event and resource markers.</p> <p>A filter form to select the categories of the events to be shown on the map and in portlets linked to the Map portlet.</p> <p>A filter form to select the capabilities of the resources to be shown on the map and in the Resources tab on the linked Details portlet. To view this form, first select View Nearby Resources on the Details portlet.</p> |
| "Details" on page 257 | <p>The Details portlet is an interactive list portlet. All the events that you are authorized to see are visible on the events list and on any map portlet linked to the Details portlet.</p> |
| "Notifications" on page 271 | <p>The Notifications portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts. For example, when related incidents occur within a defined area, an alert is sent to the Notifications portlet.</p> |
| "My Activities" on page 269 | <p>A user who is logged on can view the activities that are assigned to them in the My Activities portlet. In the My Activities portlet, the activities are grouped by their parent standard operating procedures. Each standard operating procedure corresponds to an individual event.</p> |
| "Contacts" on page 257 | <p>The Contacts portlet can display a list of your contacts that are organized by category. You can organize contacts in categories that are based on the people you need to communicate with. For example, you can have a category for general work contacts and another category for project work contacts. With the Contacts portlet, you can communicate with people and modify your online status, contacts, or groups.</p> |

Operator: Operations view

Use the Operator: Operations view to maintain awareness of events and their location. The Operator: Operations view is intended for operators, managers, or others monitoring and responding to current events.

The Operator: Operations view is an interactive web page. The page contains the portlets listed in Table 84 on page 255. The portlets are independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the operations level.

Table 84. Operator: Operations view portlets

| Portlet | Description |
|-----------------------------|--|
| “Map” on page 264 | <p>A map of the geographical region with event and resource markers.</p> <p>A filter form to select the categories of the events to be shown on the map and in portlets linked to the Map portlet.</p> <p>A filter form to select the capabilities of the resources to be shown on the map and in the Resources tab on the linked Details portlet. To view this form, first select View Nearby Resources on the Details portlet.</p> |
| “Details” on page 257 | The Details portlet is an interactive list portlet. All the events that you are authorized to see are visible on the events list and on any map portlet linked to the Details portlet. |
| “Notifications” on page 271 | <p>The Notifications portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.</p> <p>For example, when two severe events occur close together in location and time, an alert is sent to the Notifications portlet.</p> |
| “My Activities” on page 269 | A user who is logged on can view the activities that are assigned to them in the My Activities portlet. In the My Activities portlet, the activities are grouped by their parent standard operating procedures. Each standard operating procedure corresponds to an individual event. |
| “Contacts” on page 257 | The Contacts portlet can display a list of your contacts that are organized by category. You can organize contacts in categories that are based on the people you need to communicate with. For example, you can have a category for general work contacts and another category for project work contacts. With the Contacts portlet, you can communicate with people and modify your online status, contacts, or groups. |

Supervisor: Reports

Use the Supervisor: Reports view to see a summary of event data generated from running predefined reports. Also, you can use the Supervisor: Reports view to create personalized reports or configure predefined reports. These reports are intended for operators, managers, or others monitoring current events and planning future events.

The Supervisor: Reports view is an interactive web page that contains different reports based on selected data to provide you with comprehensive information and interaction at the supervisor level. This information is displayed in graphs that summarize the event data that is in the system.

In the Supervisor: Reports view, you configure and view the reports in “Reports” on page 272 portlets. By default, some of the Reports portlets display sample reports.

Operator: Reports

Use the Operator: Reports view to maintain awareness of reports, events, and alerts. The Operator: Reports view is intended for operators, managers, or others monitoring reports.

The Operator: Reports view provides a summary of event data generated from running predefined reports. You can also use the Operator: Reports view to view personalized reports. These reports help you monitor current events, take action to handle events, and plan for future events.

The Operator: Reports view is an interactive web page. You can choose to view several different reports that provide comprehensive information and interaction at the operator level.

In the Operator: Reports view, you configure and view the reports in “Reports” on page 272 portlets. By default, some of the Reports portlets display sample reports.

Location Map view

Use the Location Map view to maintain awareness of events and their position on a location map. The Location Map view is intended for operators, managers, or others monitoring and responding to current events.

The Location Map view is an interactive web page. The page contains the portlets listed in Table 85. The portlets are independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the operations level.

Table 85. Location Map view portlets

| Portlet | Description |
|----------------------------|--|
| “Location Map” on page 261 | A diagram of the location with markers for events. A filter form to select the categories of the event shown on the map. A list of the available location maps arranged by classification. |
| “Details” on page 257 | The Details portlet is an interactive list portlet. All the events that you are authorized to see are visible on the events list and on any map portlet linked to the Details portlet. |

Using portlets

A portlet provides access to information that you can view and interact with on a portal page.

The IBM Intelligent Operations Center provides several different portlets.

For help using each portlet, click the upper right corner of the portlet, and select **Help** from the menu displayed.

To resize a portlet, click the upper right corner of the portlet, and select options from the menu that is displayed, as follows:

- To expand the portlet to fill the page, click **Maximize**.
- To hide the portlet contents, other than its title bar, click **Minimize**.
- To restore a minimized or maximized portlet to its default view, click **Restore**.

Administrator

Customizing a portlet

As an administrator you can change portlet settings by clicking the upper right corner of the portlet, and selecting an option from the portlet menu.

There are two possible modes of customization, each changing the portlet settings for all users:

- **Edit Shared Settings** changes the portlet only for the instance of the portlet you are in when you change the settings.
- **Configure** changes the portlet's global settings for all instances of the portlet wherever those instances occur.

The modes of customization that are available to you depend on the permissions associated with your user ID. Global settings are superseded by shared settings.

The portlets that are supplied with the IBM Intelligent Operations Center have some settings that are specific to a portlet type, for example, set the default zoom level for a map. In addition, you can set generic portlet parameters that are common across the portlets supplied, for example, the portlet title.

Contacts

Use the Contacts portlet to send instant messages within the solution.

The Contacts portlet can display a list of your contacts that are organized by category. You can organize contacts in categories that are based on the people you need to communicate with. For example, you can have a category for general work contacts and another category for project work contacts. With the Contacts portlet, you can communicate with people and modify your online status, contacts, or groups.

Click the menus at the top of the portlet:

- **File** to add contacts, modify groups or log out
- **Tools** to set up a chat, meeting, or announcement; or to change your privacy settings
- **Help** to get more detailed information about how to use the portlet

Click your status to modify your status and message. The default status indicates that you are available. You can change your status to indicate that you are away from your computer, in a meeting, or that you do not want to be disturbed.

The status of users who are logged on is displayed in the Contacts portlet. If a user who is logged on closes the browser window or logs off from WebSphere Portal, the status of that user is still displayed as logged on until the session expires. However, any messages that are sent to that user, after the user closed the browser window, or logged off, are not delivered. Consequently, an error message is displayed to the user who is trying to send the message. To ensure that your status is updated immediately in the Contacts portlet, log off by clicking **File > Log Out**.

Note: For this portlet to work as expected, you must log on to the solution portal by using the fully qualified domain name of the IBM Intelligent Operations Center application server. If you log on to the portal by using an IP address or a host name alias instead of the registered fully qualified domain name, this portlet does not display correctly.

Administrator

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

The settings that you can change for the Contacts portlet are:

- Help file
- Portlet height
- Portlet height when maximized
- Portlet title
- Resource bundle

Related reference:

“Contacts portlet settings” on page 140

Customize the Contacts portlet by changing the settings in the fields of the **Shared Settings** window.

Details

Use the Details portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

The Details portlet is an interactive list portlet. All the events that you are authorized to see are visible on the events list and on any map portlet linked to the Details portlet.

Resources in the vicinity of an event can be displayed in a resource list and on a map.

Events and resources

The Details portlet has two interactive interface elements as shown in the following table:

Table 86. Details portlet display

| Interface element | Description |
|----------------------|---|
| Events and Incidents | The list of events contains key details for each of the events. You can display a more detailed description of an event by hovering over the row in the list. |
| Resources | The key details for the resources in the vicinity of an event are listed when you right-click the selected event. You can display a more detailed description of a resource by hovering over the row in the list. |

Initially, when you open the IBM Intelligent Operations Center the Details portlet shows all the events that are relevant to you.

In the Map portlet, you select the categories of events and the capabilities of resources to be shown. The categories of events shown on the **Events and Incidents** tab and on the Map portlet are the same. The capabilities of resources shown on the **Resources** tab and on the Map portlet are the same.

The events list is refreshed on a regular basis with new events and updates, subject to any filters you set to limit the categories shown.

A counter in the left corner of the action bar at the end of the list indicates the number of items displayed and the total number of items. In the center of the action bar, you can select the number of items to be displayed at one time. If there are more rows than can be displayed at one time, you can page forward or backward by clicking the buttons in the right corner of the action bar.

Event properties

The following table outlines the properties that describe an event:

Table 87. Event properties

| Property | Content |
|-------------------|---|
| Who | |
| Sender | Source or user ID |
| Contact name | Person to contact for additional information |
| Contact e-mail | Email address of contact person |
| Contact telephone | Telephone number of contact person |
| What | |
| Event type* | Text denoting the type of event within <i>Category</i> |
| Event status* | Event handling instructions |
| Event scope* | Intended audience for the message |
| Restriction | Additional information required when <i>Event scope</i> is 'Restricted' |
| Headline* | Short description of the event |
| Category* | High-level event classification |

Table 87. Event properties (continued)

| Property | Content |
|--------------------------|--|
| Who | |
| Severity* | Intensity of the impact of the event |
| Certainty* | Confidence in the event prediction |
| Urgency* | Timeframe for action in response to the event |
| Message type | Nature of the message |
| Description | Additional description of the event |
| Web address | Web address for additional information about the event |
| When | |
| Sent date and time | Date and time the message was submitted or sent |
| Effective date and time | Date and time the message is effective |
| Onset date and time | Date and time the event is expected to begin |
| Expiration date and time | Date and time the event is expected to end |
| Where | |
| Area description | Description of the affected area |
| Latitude / Longitude | Coordinates of the event location |

Note: Properties marked with an asterisk in the table are required for the successful creation of a new event. Properties not marked with an asterisk are optional when creating an event.

Managing events and incidents

In the Details portlet, you can perform various actions on the events in the list on the **Events and Incidents** tab. In the Map portlet, you can add an event that is shown on both the map and the events list of the Details portlet.

Procedure

On the **Events and Incidents** tab, right-click a row in the events list and select an option from the menu:

- To update the information about an event, click **Update Event**. You can enter your changes in a window with fields that contain information about the event. When an event record is updated the message type property changes to *Update*.
- To change an event status to incident, click **Escalate to Incident** to display a window and enter your contact details. When an event record is escalated there is a change to the properties and to the icon on the map.
- To remove an event from the list and the map, click **Cancel Event** to display a window and enter your contact details.
- To view the standard operating procedure (SOP) and workflow activities associated with an event, click **View Standard Operating Procedure Details**. If there are no standard operating procedures associated with an event, this option is not available. If there is an associated standard operating procedure, the Standard Operating Procedure Details window is displayed. Use the My Activities portlet to manage the workflow activities associated with a standard operating procedure.
- To view a list of the resources in the vicinity of an event, click **View Nearby Resources** and select the radius of the area you want to focus on. A list of resources is displayed on the **Resources** tab.
- To view the information about an event, click **Properties** to display a window that contains fields with information about the event.

Managing resources

You can perform various actions on the resources in the list on the **Resources** tab.

Procedure

On the **Resources** tab, right-click a row in the resources list and select an option from the menu:

- To update the information about a resource, click **Update**.
- To remove a resource from the list and the map, click **Delete**.
- To view the information about a resource, click **Properties**.

Whichever option you choose, the resource is displayed in Tivoli Service Request Manager, on the **Resources** tab. You can also view capabilities for the resource on the Tivoli Service Request Manager **Capabilities** tab. To update or delete a resource, select the resource and then select the appropriate option from the **Select Action** list.

Customizing the Details portlet

Administrator

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Set parameters for the Details portlet as follows:

By setting parameters for the Details portlet you can:

- Specify column layout, headings, sort order, and priority.
- Specify the additional conditions to filter the events or resources displayed.
- Show or hide the
 - **Add Event** button
 - **Add Resources** button
 - **Events** tab
 - **Resources** tab
 - toolbar at the top of the list.
- Specify a group name to enable communication with other map and Details portlets.
- Set the portlet to acknowledge or ignore specific types of message that come from other portlets in the group.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Related reference:

“Details portlet settings” on page 141

Customize the Details portlet by changing the settings in the fields of the **Shared Settings** window.

Key Performance Indicator Drill Down

Use the Key Performance Indicator Drill Down portlet to see more information about a KPI category, the status of its underlying KPIs.

The Key Performance Indicator Drill Down portlet shows all of the underlying KPIs associated with an organization or KPI category that is shown on the Status portlet. The KPIs are displayed in the form of a nested list that can be expanded or collapsed. The status of each underlying KPI is represented by color,

in the same way that color is used for the KPI categories that are displayed in the Status portlet. The values of the underlying KPIs control the color of the parent KPI. To display the status of the KPI, hover over the KPI with your cursor.

To focus on a specific KPI category in the Key Performance Indicator Drill Down portlet, click the category in the Status portlet. This category is then displayed on its own in the Key Performance Indicator Drill Down portlet. You can use the list to inspect the underlying KPIs until you reach details of the KPI that caused the status change.

Administrator

Customizing the Key Performance Indicator Drill Down portlet

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

By setting parameters for the Key Performance Indicator Drill Down portlet you can:

- Specify column layout, headings, sort order, and priority.
- Customize KPI colors.
- Enable an additional KPI filter.
- Show or hide the toolbar at the top of the list.
- Specify a group name to enable communication with a Key Performance Indicator Drill Down portlet.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Related concepts:

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

Related reference:

“Key Performance Indicator Drill Down portlet settings” on page 145

Customize the Key Performance Indicator Drill Down portlet by changing the settings in the fields of the **Shared Settings** window.

Location Map

Use the Location Map portlet to see events marked on a location map. A location map in the IBM Intelligent Operations Center is a map or plan with predefined areas for interaction, for example, seating areas in a major sports stadium.

The Location Map portlet provides you with a visual representation of events in the position they occur. The Location Map portlet together with Map, and Details portlets enable you to identify issues, location patterns, conflicts, and synergies.

The Location Map, Map, and Details portlets can be linked together to share input and changes to the events displayed. You can select in the Location Map portlet the categories of events you want to view. Your selection affects the events displayed in the Location Map portlet and the Map and Details portlets that are linked to it.

Location Map interface

The Location Map portlet has three interactive interface elements as shown in the following table:

Table 88. Location Map portlet interface elements

| Interface element | Description |
|----------------------------------|---|
| Location map | A diagram of the location with markers for events. |
| Select Content: Event Categories | A filter form to select the categories of the event shown on the map. |
| Map menu | A list of the available location maps arranged by classification. |

Initially, the portal page opens with the Location Map portlet and all the events that are relevant to you are displayed on the location map. The map is updated with new events, subject to any filters you set to limit the categories shown. A menu bar listing all the available maps is provided to the left of the map.

An event that occurs in an area is represented by a marker at the corresponding position on the location map. You can display an event headline and description by hovering over the event marker on the map. The window includes the name and description of the area in which the event occurs. If more than one event occurs in the same area, the events are clustered and represented by a cluster marker. When you hover over this marker, the headline of each event is included in the window. You can also display an area name and description by hovering over any of the predefined areas in the map that are without events.

Where portlets are linked, you can click an event in this portlet and corresponding events in other portlets in the group are selected also. Similarly, selecting an event in any one of the linked portlets results in that event highlighted in this portlet.

Note: An event must have an area identifier to be shown on the Location Map portlet. In addition, an event must have latitude and longitude coordinates to be shown on both the Location Map and the Map portlets. If an event does not have area identifier or coordinates, it can be shown only on the Details portlet.

Map markers

The map represents the location of events with one of the following types of marker:

Table 89. Map markers

| Marker Type | Description |
|-------------|---|
| Icon | Pinpoints on the map the position of an event with a unique icon for each category of event. |
| Cluster | Indicates more than one event in the same area with a number that represents the number of events in that area. |

The icon that represents an event type is defined in the category field of the event details on the **Events and Incidents** tab in the Details portlet. When an event is escalated to an incident, the icon displayed on the map retains its category-specific symbol, with the addition of a red margin around the icon.

Map controls

You can move the cursor around the map by using your mouse or keyboard.

The map controls are on the upper left side of the map

The map controls are on the upper left side of the map. They consist of:

- Pan arrows (up, down, left, right)
- Zoom in
- World view (zooms out to the maximum extent)
- Zoom out

Pan controls for moving around the map

To move around the map you can:

- Click and drag the map by using the mouse
- Press the up pan arrow, or the up arrow key on the keyboard, to pan north
- Press the down pan arrow, or the down arrow key on the keyboard, to pan south
- Press the right pan arrow, or the right arrow key on the keyboard, to pan east
- Press the left pan arrow, or the left arrow key on the keyboard, to pan west

Zoom controls for magnifying or reducing the scale of the map

To zoom in and out of the map you can:

- Click the + map icon to zoom in, or the - map icon to zoom out of the center of the map
- Double-click the mouse to center the map and zoom in to the selected location
- Click the **World view** icon to maximize the zoom out to show the world view
- Press the + key on the keyboard to zoom in
- Press the - key on the keyboard to zoom out
- Press Shift while you use the mouse to draw a rectangle around the area to zoom in on

Selecting event categories for the map

With the Event Categories filter, you can select by category which events are displayed on the map.

To view the filter form, click **Select Content**. The categories of events displayed on the map, and in associated portlets, can be changed based upon the filter form selection here. You can focus on the categories of event you want to analyze by using the filter to hide the event categories you do not need. The map responds to any change on the filter form. When the selection is changed, the map is updated and only the positions of events within the selected categories are plotted on the map. Change the categories of event displayed by selecting or clearing check boxes on the filter form. To close the filter form, click **Select Content**. If you leave the portal page and return, the filter is reset to the default selection.

You can focus on individual events you want to analyze by selecting check boxes in the Details portlet. These events are then also highlighted in linked portlets.

Customizing the Location Map portlet

Administrator

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Map and Location Map portlets can also be customized by changing global settings. Global settings affect the content of the portlet for all users and for all occurrences of the portlet. Global settings are superseded by shared settings.

The settings you can change for Location Map portlet are as follows:

- The default selection on the Event Categories filter
- The name of the default location map to be displayed
- The default area highlight color, when you use the cursor to hover over an area.
- The name of the group that enables communication with other map and Details portlets

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Customizing location maps

You can use the Location Map Manager portlet to customize the following aspects of the Location Map portlet:

- Classification name to be displayed on the menu on the left of the portlet.
- Map to be displayed in the portlet.
- Areas within a map.

Related concepts:

“Location Map Manager” on page 168

Use the Location Map Manager portlet to customize the Location Map portlet.

Related reference:

“Location Map portlet settings” on page 148

Customize the Location Map portlet by changing the settings in the fields of the **Shared Settings** window.

Map

Use the Map portlet to see events and resources on a map.

The Map portlet provides you with a visual representation of events and resources on a map. Use the Map portlet together with the Location Map and the Details portlets, to identify location patterns, conflicts, issues, and synergies.

The Map, Location Map, and Details portlets can be linked together to share input and changes to the events displayed. You can select in the Map portlet the categories of events and the capabilities of resources you want to view. Your selection affects what is displayed in the Map portlet and in the linked Location Map and Details portlets.

Map interface

The Map portlet has three interactive interface elements as shown in the following table:

Table 90. Map portlet interface elements

| Interface element | Description |
|----------------------------------|--|
| Map | A map of the geographical region with event and resource markers. |
| Select Content: Event Categories | A filter form to select the categories of the events to be shown on the map and in portlets linked to the Map portlet. |
| Select Content: Resources | A filter form to select the capabilities of the resources to be shown on the map and in the Resources tab on the linked Details portlet. To view this form, first select View Nearby Resources on the Details portlet. |

Initially, the portal page opens with the Map portlet and all the events that are relevant to you on the map. If an event has latitude and longitude values specified, you can see the event location in the form of an icon marker on the map. You can display an event headline and description by hovering over the event marker on the map. If there is more than one event clustered at the same location, the number of events is indicated on the marker. When you hover over that cluster marker, the headline of each event is included in the window. The map is updated with new events, subject to any filters you set to limit the categories shown.

Where portlets are linked, you can click an event marker in one portlet and the corresponding event in the other portlets in the group are selected also.

There is a limit to the number of markers that can be shown on the map. If the number of markers in the area in view exceeds the threshold, the markers are not shown. You receive a message with the number of markers available and the number of the threshold. You are given two options to display all available markers:

- Zoom in or pan to an area of the map with the number of markers below the threshold.
- Click **Load all items in view**.

If you choose the second option, you might notice that markers appear on the map at a slower rate. There is a third option: use the filter to select fewer categories.

When you select **View Nearby Resources** for an event in the Details portlet, resources are shown on the map based on the radius and capabilities you selected.

The map keeps you up-to-date by adding new events to the map, subject to any filters you set to limit the categories shown.

Note: If an event has an area identifier in addition to latitude and longitude coordinates, it can be shown on both the Location Map and the Map portlets. All events can be shown on the Details portlet.

Map markers

The map represents the location of events or resources with one of the following types of marker:

Table 91. Map markers

| Marker Type | Description |
|-------------|--|
| Icon | pinpoints on the map the location of an event or a resource on the map with a unique icon for each category or resource type |
| Polygon | outlines on the map the area associated with a particular event |
| Cluster | indicates more than one event at the same location with a number that represents the number of events at that location |
| Radius | outlines on the map the area you select for View Nearby Resources in relation to an event |

The icon that represents an event type is defined in the category field of the event details on the **Events and Incidents** tab in the Details portlet. When an event is escalated to an incident, the icon displayed on the map retains its category-specific symbol, with the addition of a red margin. Clicking an event marker on the map highlights the associated event or events in the Details portlet.

The icon that represents a resource is defined in the type field of the resource details on the **Resources** tab in the Details portlet. To view resource icons, first select **View Nearby Resources** on the Details portlet.

Using the map controls

You can move the cursor around the map by using your mouse or keyboard.

The map controls are on the upper left side of the map

The map controls are on the upper left side of the map. They consist of:

- Pan arrows (up, down, left, right)
- Zoom in
- World view (zooms out to the maximum extent)
- Zoom out

Pan controls for moving around the map

To move around the map you can:

- Click and drag the map by using the mouse
- Press the up pan arrow, or the up arrow key on the keyboard, to pan north
- Press the down pan arrow, or the down arrow key on the keyboard, to pan south
- Press the right pan arrow, or the right arrow key on the keyboard, to pan east
- Press the left pan arrow, or the left arrow key on the keyboard, to pan west

Zoom controls for magnifying or reducing the scale of the map

To zoom in and out of the map you can:

- Click the + map icon to zoom in, or the - map icon to zoom out of the center of the map
- Double-click the mouse to center the map and zoom in to the selected location
- Click the **World view** icon to maximize the zoom out to show the world view
- Press the + key on the keyboard to zoom in
- Press the - key on the keyboard to zoom out
- Press Shift while you use the mouse to draw a rectangle around the area to zoom in on

Selecting event categories for the map

Use the Event Categories filter to select by category which events are displayed on the map.

To view the filter form, click **Select Content**. The categories of events displayed on the map portlet can be changed based upon the filter form selection that you make. You can focus on the categories of event you want to analyze by using the filter to hide the event categories you do not need. The map responds to any change on the filter form. A change on the filter form also affects other portlets in the same group. When a selection is changed, the map is updated and only the locations of events within the selected categories are plotted on the map. Change the categories of event displayed by selecting or clearing check boxes on the filter form. To close the filter form, click **Select Content**. If you leave the portal page and return, the filter is reset to the default which is all categories selected.

You can focus on individual events you want to analyze by ticking check boxes in the Details portlet. These events are highlighted on the map.

Selecting resource capabilities for the map

When you select **View Nearby Resources** on the Details portlet, the Event Categories filter is replaced by the Resources filter. Use the Resources filter to select by capability which resources are displayed on the map.

To view the filter form, click **Select Content**. The capabilities of resources displayed on the map and in the Details portlet can be changed based upon the filter form selection that you make. You can focus on the capability you want to analyze by using the filter to hide the capabilities you do not need. The map responds to any change on the filter form. A change on the filter form also affects the Details portlet in the same group. When a selection is changed, the map is updated and only the locations of the resources with the selected capabilities are plotted on the map. Change the capability of resources displayed by selecting or clearing a check box on the filter form. To close the filter form, click **Select Content**. If you leave the portal page and return to the resources filter form, the filter is reset to default which is all capabilities selected. The capabilities selected by default depend on the category of the event and how that category is mapped to capabilities.

Resetting the map

The Map portlet can be reset to the default view configured for the IBM Intelligent Operations Center.

Procedure

1. On the Map portlet, click **Reset the Map** or click the arrow in the upper right corner.
2. Select one of the following options:
 - **Reset the Map** to zoom and center the map to the default setting.
 - **Reset the Map and Clear Filters** to zoom and center the map to the default setting and reset the values set in **Select Content** to the default values.

Results

The map is reset according to the option selected, but only for the current user and view.

Adding an event

You can create an event, adding it to the Map portlet map and the Details portlet list at the same time. The map and the list provide two ways of looking at the same content.

About this task

Use the **Add Event** dialog to specify event properties, as outlined in the following table:

Table 92. Event properties

| Property | Content |
|-------------------|---|
| Who | |
| Sender | Source or user ID |
| Contact name | Person to contact for additional information |
| Contact e-mail | Email address of contact person |
| Contact telephone | Telephone number of contact person |
| What | |
| Event type* | Text denoting the type of event within <i>Category</i> |
| Event status* | Event handling instructions |
| Event scope* | Intended audience for the message |
| Restriction | Additional information required when <i>Event scope</i> is 'Restricted' |
| Headline* | Short description of the event |
| Category* | High-level event classification |
| Severity* | Intensity of the impact of the event |
| Certainty* | Confidence in the event prediction |

Table 92. Event properties (continued)

| Property | Content |
|--------------------------|--|
| Who | |
| Urgency* | Timeframe for action in response to the event |
| Message type | Nature of the message |
| Description | Additional description of the event |
| Web address | Web address for additional information about the event |
| When | |
| Sent date and time | Date and time the message was submitted or sent |
| Effective date and time | Date and time the message is effective |
| Onset date and time | Date and time the event is expected to begin |
| Expiration date and time | Date and time the event is expected to end |
| Where | |
| Area description | Description of the affected area |
| Latitude / Longitude | Coordinates of the event location |

Procedure

1. Right-click a location on the map and click **Add Event** to launch the **Add Event** dialog. Some of the event properties are completed automatically.
2. Specify the remaining event properties, in the fields in the dialog. Properties marked with an asterisk are required for the successful creation of a new event. Those properties not marked with an asterisk are optional.
3. Click **OK** to save the event or **Cancel** to stop adding the event.

Results

An icon that represents the category of the new event is displayed in the requested location on the map. You can see the details of the new event in the linked Details portlet list.

Customizing the Map portlet

Administrator

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

Map and Location Map portlets can also be customized by changing global settings. Global settings affect the content of the portlet for all users and for all occurrences of the portlet. Global settings are superseded by shared settings.

You can change the following settings specific to the Map portlet:

- Reset the default center point and zoom level for the map.
- Select a new base map, the default is an ArcGIS map supplied by Esri.
- Add to the map geographic annotation and visualization layers in KML (Keyhole Markup Language), to represent additional data.
- Set a threshold for the number of markers that can be displayed without a warning message.
- Set the default selection on the map filters, to be displayed when you click **Select Content**.

- Specify the name of the group that enables communication with other map and Details portlets

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Related reference:

“Map portlet settings” on page 150

Customize the Map portlet by changing the settings in the fields of the **Shared Settings** window.

My Activities

The My Activities portlet displays a dynamic list of activities that are owned by the group of which the user, who is logged on to the interface, is a member.

Each time an event triggers a standard operating procedure according to the selection criteria defined in the standard operating procedure selection matrix, the associated activities are assigned to owners. For more information about standard operating procedures, see the link at the end of the topic.

A user who is logged on can view the activities that are assigned to them in the My Activities portlet. In the My Activities portlet, the activities are grouped by their parent standard operating procedures. Each standard operating procedure corresponds to an individual event.

For each standard operating procedure, the My Activities portlet displays only open activities, and not closed or completed activities. Open activities include those activities that are already started, and those activities that are eligible to be started. For example, if one or more of the activities that are specified in a standard operating procedure are ordered in a sequence, only the current activity in the sequence is displayed. If a particular activity relies on the completion of a predecessor activity, it is not displayed until the predecessor activity is complete or skipped.

The following activity due icons are displayed near the top of the My Activities portlet:

Past Due

Activities whose completion is past due.

Today Activities that are due to be completed today.

Future Activities whose completion is due in the future.

When an activity is started, the due date is calculated by adding the start time to the duration of the activity. The activity due dates are used to calculate the number that is displayed in each of the activity due icons.

In the My Activities portlet, standard operating procedures that have past due activities are displayed first, and the remaining standard operating procedures are displayed in alphabetical order.

Next to each standard operating procedure in the list that has past due activities, a red icon indicates the number of activities that are past due. The standard operating procedures with past due activities are sorted according to the number of past due activities they contain. The standard operating procedure that has the most past due activities is displayed at the top of the list.

Managing activities in the My Activities portlet

Manage your activities in the My Activities portlet:

- To view details about a standard operating procedure, expand the name of the standard operating procedure.
 - The name of the event that triggered the standard operating procedure is displayed. Hover over the event name to view hover help information that includes the event start date and time, and the category, severity, certainty, and urgency of the event.

- If the Details portlet is displayed on the page, to view the event properties, click the event name. The event Properties window is displayed.
- Steps that are in progress or eligible to be started are displayed. Also, the status and due date of each step is displayed.
- To view further details about a step, including comments and references that users added to the step, expand the name of the step.
- To start, finish, or skip a step, expand the name of the step, and then choose one of the following options:
 - To start a step, from the list, select **Start**. If the step is defined as an automated task in the standard operating procedure, the workflow that is assigned to the task is started automatically, and the step is finished automatically. The user who starts a step becomes the owner of that step, and the name of the user is displayed in the **Owner** field.
 - To skip a step, from the list, select **Skip**.
 - To finish a step, from the list, select **Finish**.
- To add a comment to a step, use the following substeps:
 1. Expand the name of the step.
 2. From the list, select **Add Comment**.
 3. In the Add Comment window, enter a comment in the **Comment** field. **Commentator name** and **Activity name** are read-only fields and contain automatically entered values.
 4. Click **OK**.
 5. Expand the name of the step again. The new comment is displayed at the end of the list of existing comments and references for the step.
- To add a reference to a step, use the following substeps:
 1. Expand the name of the step.
 2. From the list, select **Add Reference**.
 3. In the Add Reference window, enter values for **Reference name** and **Reference URI**. **Activity name** is a read-only field that contains an automatically entered value.
 4. Click **OK**.
 5. Expand the name of the step again. The new reference is displayed as a link at the end of the list of existing comments and references for the step.
- To view the details for a standard operating procedure, click the **i** icon next to the name of the standard operating procedure. In the Standard Operating Procedure Details window, all the activity steps that are included in the standard operating procedure are displayed, including those steps that are in progress, eligible to be started, completed, and closed. The status and due date of each step is also displayed. To view further details about a step, expand the step name.

Administrator

Customizing the My Activities portlet

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

For the My Activities portlet, you can specify a group name to enable communication with other portlets; for example, Details portlets.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Related concepts:

“Standard Operating Procedures” on page 123

You can define standard operating procedures and activities to manage events that come into the IBM Intelligent Operations Center. Use the Standard Operating Procedures portlet to access the standard operating procedure, standard operating procedure selection matrix, and workflow designer applications in Tivoli Service Request Manager.

Related reference:

“My Activities portlet settings” on page 152

Customize the My Activities portlet by changing the settings in the fields of the **Shared Settings** window.

Notifications

Use the Notifications portlet to view your alert messages and their details.

The Notifications portlet is an interactive window that contains a list of all the current alerts relevant to you. You see those only alerts sent to the user groups you are a member of. Alerts are notifications that received when:

- Multiple events are happening in the same vicinity and at a similar time, thus might be in conflict or require coordination
- A predefined key performance indicator (KPI) value change occurs, where that change is defined as an alert trigger by your administrator

You can also use the portlet to display further details of an alert.

Notifications list

The Notifications portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.

To show a more detailed description of an alert, hover over the row with the cursor. To see all the information that is associated with that alert in a window, right-click the row and select **Properties**.

Initially, when you open the portal page, the portlet displays all of your current alerts. Remove any alert from the portlet by right-clicking the row and selecting **Close alert**. It is possible to close multiple alerts in this way by selecting multiple rows. Close an alert only after you have handled it appropriately because the alert is removed for all recipients when you close it.

Click the button in the upper right corner of the window to cancel it and take you back to the list.

A counter in the left corner of the action bar at the end of the list indicates the number of items displayed and the total number of items. In the center of the action bar, you can select the number of items to be displayed at one time. If there are more rows than can be displayed at one time, you can page forward or backward by clicking the buttons in the right corner of the action bar.

Alert Properties

The window for alert details displays the following properties:

Table 93. Alert properties

| Property | Content |
|----------|---|
| Headline | Short description of the alert |
| Category | High-level classification of event or KPI |
| Sender | Source of the alert |

Table 93. Alert properties (continued)

| Property | Content |
|------------------|---|
| Sent to Groups | Groups to whom the alert was sent |
| Sent | Date and time the alert was sent |
| Description | Additional description of the alert |
| Refers to Alerts | Event identifier, if the alert is caused by correlated events |
| Refers to KPIs | Name of the KPI, if the alert is caused by a changing KPI value |

Administrator

Customizing the Notifications portlet

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

By setting parameters for the Notifications portlet you can:

- Specify column layout, headings, sort order, and priority.
- Show or hide the toolbar at the top of the list.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Related reference:

“Notifications portlet settings” on page 153

Customize the Notifications portlet by changing the settings in the fields of the **Shared Settings** window.

Reports

Use the Reports portlet to view a report of events as a graph. The portlet provides various options to group events by, and you can choose events by a particular date or date range. These reports help you plan responses to current and future events.

Creating reports

You can create a custom report for events using the Reports portlet. Begin by selecting how you want to group events. For example, to view all events by a particular category, select **Category** in the **Group by** field. Then in the **Select data** fields, choose the data specific to the information that you want to view. You can also indicate a date or range of dates for the events on the report. Click **Update**, and the graph changes to reflect the information you requested.

To retrieve the URL for the new report, click **URL For This Report**.

Table 1 shows the options by which you can group events.

Table 94. Custom report

| Group by | Description |
|------------|---|
| Event Type | Displays events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| Severity | Displays events based on severity. For example, events might be extreme or severe. |

Table 94. Custom report (continued)

| Group by | Description |
|----------------|---|
| Certainty | Displays events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Urgency | Displays events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Event Category | Displays events based on event category. For example, you can view all environmental, fire, or transportation events. |
| Message Type | Displays events based on message types such as updates and alerts. |
| Status | Displays events by status. The statuses are: <ul style="list-style-type: none"> • Acceptable • Caution • Take action |
| Sender | Displays events by a particular sender. For example, the event might be a security issue or an issue that affects IBM Intelligent Operations for Water. |
| Incident | Displays events based on the type of incident. For example, you can display all traffic accidents or all road construction. |
| Handling Code | Displays events by handling code. For example, the handling code might be "event." |
| Sender Name | Displays events by the sender's name. |

Table 2 shows the data that you can select for the report.

Table 95. Select data

| Select Data | Description |
|----------------|--|
| Severity | Displays events based on severity. For example, events might be extreme or severe. |
| Certainty | Displays events based on how likely they are to occur. For example, if a traffic accident occurred, the certainty might be "observed." |
| Urgency | Displays events based on how urgent they are. For example, the event might be occurring and described as "immediate." |
| Event Category | Displays events based on event category. For example, you can view all environmental, fire, or transportation events. |
| Event Type | Displays events based on type. For example, the event might be a tornado approaching or a traffic accident. |
| From Date | Enter the date for which you are viewing events. For a range of dates, enter the beginning date. |
| To Date | Enter the date through which you are viewing events. |

Note: For this portlet to work as expected, you must log on to the solution portal by using the fully qualified domain name of the IBM Intelligent Operations Center application server. If you log on to the portal by using an IP address or a host name alias instead of the registered fully qualified domain name, this portlet does not display correctly.

Copying a report URL

To copy a report URL and have the report display in a frame on the right side of the portlet, right-click on the URL and select **Copy link address**. The wording for the **Copy link address** option varies depending on your browser.

Important:

To save a user-defined report and use the link you copied here, enter yesterday's date in the **From Date** field and tomorrow's date in the **To Date** field. These dates ensure that you get all of the data that you want included on the user-defined report. For example, for the date range 8/10/2012 through 8/18/2012, enter the following dates for the filter criteria:

- From Date - enter 8/9/2012
- To Date - enter 8/19/2012

Report samples

The IBM Intelligent Operations Center has a Reports portlet that contains graphical reports based on the Events portlet data.

The large report frame is where you select the parameters for the information that appears on the report graph.

The two frames along the right side of the portlet are where user-defined reports are copied into.

The reports along the bottom of the page are predefined charts. To configure these reports to show events by a date or date range, click **Configure the Report**. Enter the dates, and click **View the Report**.

Integrating your reports

The Reports portlet provides an IFrame to embed IBM Cognos Business Intelligence reports or pages. You specify the URL to the report or page that you want to integrate with the portlet.

Administrator

Customizing the Reports portlet

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet width, and portlet title. You can also specify the URL of the report that is displayed.

Related reference:

“Reports portlet settings” on page 154

Customize the Reports portlet by changing the settings in the fields of the **Shared Settings** window.

Status

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary.

KPI color code

Each column contains KPI information about an organization that is named at the top of the column. The KPI categories that are associated with each organization are represented by colored cells. The background color for a KPI category reflects its status. If there are more than six KPIs to be displayed in a column, the size of each individual cell is reduced to accommodate the extra KPIs.

The background color code that is supplied with the solution's sample KPIs is as follows:

- Green indicates that the status is acceptable, based on the parameters for that KPI.
- Yellow indicates that caution or monitoring is required.
- Red indicates that action is recommended.
- Gray indicates that there is insufficient data available to calculate the KPI status.

The color code is defined in the legend at the top of the portlet.

An undetermined status indicates that there is no KPI value available in the time period that is defined for that KPI. This situation occurs when the solution does not receive any messages for the KPI in the specified time period. For example, the water level for a water source is calculated daily. If no water level message for that water source is received on a particular day, then there is no data to determine the KPI value.

To see the KPI name and a definition of the status that is represented by the color of a KPI, hover over the cell with your cursor.

KPI updates

When an underlying KPI changes, the change is reflected in the Status portlet. For example, one of the sample KPIs that determine the status of the Water Quality KPI changes status from acceptable to caution. The change is reflected in the portlet by a change in the background color of the Water Quality cell from green to yellow. In addition, the Notifications portlet indicates that a KPI changed.

When the solution receives a message that is related to the calculation of a KPI, there is an instant color change. This feature is an advantage when the KPI category is one that is likely to receive changes in real time, for example, airport delays. It is not relevant to those categories that contain historical KPIs, for example, flood control. For those categories of KPI, regular daily measurements are taken and there is unlikely in the interim to be a sudden change that affects status.

For each KPI, you can see all of the underlying KPIs and details in the Key Performance Indicator Drill Down portlet that is linked to the Status portlet.

To focus only on a specific KPI in the Key Performance Indicator Drill Down portlet, click the KPI cell in the table in the Status portlet. You can also click the owning organization title, for example, for example "Water", to see all related KPIs.

Administrator

Customizing the Status portlet

If you have administrator access, you can customize this portlet. Click the button in the upper right corner of the portlet to see your portlet menu customization options. Shared settings affect the content of this portlet for all users, but only for this occurrence of the portlet.

By setting parameters for the Status portlet you can:

- Customize KPI colors.
- Enable an additional KPI filter.
- Show or hide the KPI legend.
- Define how the KPIs are sorted.
- Specify a group name to enable communication with a Key Performance Indicator Drill Down portlet.

You can set generic portlet parameters that are common across portlets: help file location, portlet height, portlet title, and resource bundle.

Customizing KPIs

A set of sample KPIs is provided with the solution. These KPIs are designed to provide guidance for planning and implementing different types of KPIs to suit your organization. Examples are provided in the areas of water, transportation, and public safety.

Related concepts:

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

Related reference:

“Status portlet settings” on page 156

Customize the Status portlet by changing the settings in the fields of the **Shared Settings** window.

Chapter 9. Troubleshooting and support

To isolate and resolve problems with your IBM software, you can use the troubleshooting and support information, which contains instructions for using the problem-determination resources that are provided with your IBM products.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels

of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to surface?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve. However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Related information

“Searching knowledge bases” on page 305

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

Enabling traces and viewing log files

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics give some guidance on how to access log files.

To start the traces and view the logs, enter the commands at run time as the root user.

Related concepts:

“Verifying the components” on page 199

The System Verification Check tool tests components within IBM Intelligent Operations Center to determine if they are accessible and operational.

“Installing and using IBM Support Assistant Lite” on page 287

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

Related tasks:

“Running the installation must gather tool” on page 283

Log files are generated while IBM Intelligent Operations Center is installed. A tool is available to gather these log files for analysis.

Application server log files

Use the following procedures to enable traces and view logs for some of the systems on the application server.

The following procedures describe how to enable traces and view logs for the following systems:

- WebSphere Portal
- IBM WebSphere Business Monitor

Enabling tracing and viewing logs on WebSphere Portal

About this task

WebSphere Portal logs are at `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal`. Follow the steps in the procedure to start a trace and view a log.

Procedure

1. Log on to the administrative console at `http://app-host:9060/ibm/console`, where **app-host** is the fully qualified host name of the application server.
2. Click **Troubleshooting > Logs and Trace**.
3. Click **WebSphere_Portal > Change log level details**.
4. Click the **Runtime** tab and paste in the following command:

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

5. Click **OK**.

6. To view a log, enter the following commands:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

Enabling tracing and viewing logs for IBM WebSphere Business Monitor on the application server

About this task

Logs for IBM WebSphere Business Monitor on the application server are located at `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/`. Follow the steps in the procedure to start a trace and view a log.

Procedure

1. Log on to the administrative console at `http://app-host:9060/ibm/console`, where **app-host** is the fully qualified host name of the application server.
2. Click **Troubleshooting > Logs and Trace**.
3. Click **WBM_DE.AppTarget.WBMNode1.0 > Change log level details**.
4. Click the **Runtime** tab and paste in the following trace level code: `*=info: com.ibm.wbm.*=finest:
com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all:
com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Click **OK**.

Related information:

 [IBM WebSphere Portal 7 Product Documentation](#)

Event server log files

Use the following procedures to enable traces and view logs for some of the systems on the event server.

The following procedures describe how to enable traces and view logs for the following systems:

- Tivoli Service Request Manager
- WebSphere MQ and WebSphere Message Broker
- Tivoli Netcool/OMNIBus XML probe
- Tivoli Netcool/OMNIBus (object server) database
- Tivoli Netcool/OMNIBus (Process Agent) Database
- Tivoli Netcool/Impact

Enabling tracing and viewing log files for Tivoli Service Request Manager

About this task

Use the following procedure to debug the flow of information from Tivoli Service Request Manager to IBM Intelligent Operations Center.

Procedure

1. In the Tivoli Service Request Manager user interface, click **Go To > System configuration > Platform Configuration > Logging**.
2. Under **Root Loggers**, in the filter field, enter `integration`.
3. Expand **integration**.
4. Configure the integration logger:
 - a. For **Log Level**, click the **Select Value** icon. In the Select Value window, click **DEBUG**.
 - b. For **Appenders**, click the **Manage Appenders** icon. In the Manage Appenders window, select the **Dailyrolling** check box, and then click **OK**.
 - c. Select the **Active?** check box.
 - d. Click the **Save Logger** icon.
5. From the **Select Action** list, select **Set Logging Root Folder**.
6. In the Set Logging Root Folder window, for **Root Logging Folder**, enter `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1`, and then click **OK**.
7. Click the **Save Logger** icon.
8. From the **Select Action** list, select **Apply Settings**.
9. To view the log, in a Tivoli Service Request Manager server terminal, enter the following commands:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs  
tail -f event-host_MXServer_maximo_scheduled.log
```

where *event-host* is the hostname of the event server.

Related tasks:

“Checking the log files” on page 320

Check the Tivoli Netcool/OMNIbus policy log file, and the Tivoli Service Request Manager log file.

Enabling tracing and viewing log files for WebSphere MQ and WebSphere Message Broker

About this task

Logs for WebSphere MQ and WebSphere Message Broker are stored at the following locations:

- /var/mqm/errors
- /var/mqm/qmgrs/IOC!MB!QM/errors

Trace files are written to the /var/mqm/trace directory. You can turn on tracing for a single queue manager or all queue managers, as shown in the following procedure.

Procedure

1. To start, end, or format a trace, choose the appropriate command:
 - To start a trace for all processes, enter the following command: `strmqtrc -e`
 - To start a trace for the IBM Intelligent Operations Center queue manager, enter the following command: `strmqtrc -m IOC.MB.QM`
 - To start a high detail trace for the IBM Intelligent Operations Center queue manager, enter the following command: `strmqtrc -t all -t detail -m IOC.MB.QM`
 - To end all tracing, enter the following command: `endmqtrc -a`
 - To format the binary trace files in ASCII format, enter the following command: `dspmqrtrc *.TRC`
2. To check the status of WebSphere Message Broker:
 - a. Enter the following command: `ps -ef | grep IOC_BROKER`
 - b. Check the status of the following processes:
 - `bipservice IOC_BROKER`
 - `bipbroker IOC_BROKER`
 - `biphttplistener IOC_BROKER`
 - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

Enabling tracing and viewing log files for the Tivoli Netcool/OMNIbus XML probe

About this task

WebSphere Portal logs are located at /opt/IBM/netcool/omnibus/log/ioc_xml.log. Follow the steps in the procedure to start a trace and view a log.

Procedure

1. Open a terminal on the event server.
2. Enter the following command: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
3. If the Connection status OK message is not displayed at the bottom of the file, to rename the current log file, enter the following command: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. If the Connection status OK message is not displayed, you might also see the message Probe shutting down. To restart the probe, enter the following command:
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
5. After approximately 1 minute, enter the following command again: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`

6. If the Connection status OK message is still not displayed, check the `/opt/IBM/netcool/omnibus/log/ioc_xml.log` file for errors. A connection problem might mean that the object server is down. See the following section, *Enabling tracing and viewing logs for the Tivoli Netcool/OMNIBus (object server) database*.

Enabling tracing and viewing log files for the Tivoli Netcool/OMNIBus (object server) database

About this task

The log files are located at the following locations:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`, for example:
 - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
 - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
 - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`

Follow the steps in the procedure to start a trace and view a log.

Procedure

1. Log on to a terminal as a root user.
2. Enter the following command: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. If you are asked do you want to import from `omni.dat`, click **yes**, and then click **finish**.
4. Minimize the process agent window.
5. Right-click **NCOMS**.
6. Choose the appropriate option:
 - If the **Connect As...** option is not displayed, you must start the NCOMS object server:
 - a. To start the NCOMS object server, close `nco_config` and enter the following command:
`/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
 - b. If the NCOMS object server does not start, look for a `NCOMS.pid` file in the `/opt/IBM/netcool/omnibus/var` directory and delete it, then try to start the server again.
 - If the **Connect As...** option is displayed, click **Connect As...**, then for user name, enter `root`, and enter the password.
7. Once you have started the NCOMS server, to restart the probe, enter the following command:
`/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
8. To view the log file, enter the following command: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

Tivoli Netcool/OMNIBus (Process Agent) Database log file

The Tivoli Netcool/OMNIBus (Process Agent) Database log file is located at `/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

Enabling and viewing Tivoli Netcool/Impact log files

About this task

The log file is located at `opt/IBM/netcool/impact/log/`. Follow the steps in the procedure to start a trace and view a log.

Procedure

1. Log on to the Tivoli Netcool/Impact administrative console at `http://event-host:9080/nci` with the user name `admin`, where `event-host` is the fully qualified host name of the event server. If a login prompt is not displayed, enter the following commands in a terminal window:

```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```

2. In the Service Status window, scroll down and make sure that the following services are running, as indicated by a green symbol:
 - IOC_CAP_Event_Reader
 - IOC_Notification_Reader
3. Also in the Service Status window, click the **View Log** icon next to **PolicyLogger** to see if there are any errors displayed in the log.
4. If there are one or more errors in the log, for more details see the log files in the following directory:
/opt/IBM/netcool/impact/log/
5. If you need more details, set the log levels higher. Click **PolicyLogger**, and then set the value of **Highest log level** to 3 and select the appropriate check boxes.

What to do next

You can turn on various logs at run time through the WebSphere Application Server administrative console. For more information about turning on portal tracing and other traces that are available from WebSphere Portal, see the link near the start of the topic for the WebSphere Portal product documentation and search for *Logging and tracing*.

Related tasks:

“Checking the log files” on page 320

Check the Tivoli Netcool/OMNIBus policy log file, and the Tivoli Service Request Manager log file.

Running the installation must gather tool

Log files are generated while IBM Intelligent Operations Center is installed. A tool is available to gather these log files for analysis.

Procedure

1. Log on the installation server as root and open a terminal window.
2. Change to the *install_home/ioc/bin* directory.
3. Run the **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** command to set the JAVA_HOME variable to use the Java 6 runtime JRE.
4. Run the **./mustgather.sh -p password** command where *password* is the topology password. The tool scans the topology properties file the first time it is run. If the topology properties file is changed after running the tool, add **-n** to the command to have the tool re-scan the topology properties file. For example, **./mustgather.sh -n -p password**.

Results

The collected logs and other information are written to the *install_media/mustGather* directory on the installation server. There will be one file with a *.tar* extension for each of the servers.

Collected information includes:

- Logs for all installation phases including logs for each component installed on each node.
- System Verification Check tool installation logs.
- The topology XML files.
- All scripts used during the installation process.
- All vulnerabilities address by cyber hygiene.
- The cyber hygiene scripts.

Related concepts:

“Enabling traces and viewing log files” on page 279

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics give some guidance on how to access log files.

“Troubleshooting the components”

You can use the System Verification Check tool to troubleshoot components in the IBM Intelligent Operations Center.

Related tasks:

“Restarting the IBM Intelligent Operations Center architecture installation during a step-by-step installation” on page 46

If the architecture installation fails, the installation can be restarted.

“Exchanging information with IBM” on page 309

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Troubleshooting the components

You can use the System Verification Check tool to troubleshoot components in the IBM Intelligent Operations Center.

For more information about the System Verification Check tool, see the link at the end of the topic.

The tables in the following sections lists the log file locations for each of the servers contained in IBM Intelligent Operations Center. All the log files are created automatically. View them using the appropriate tail commands.

Installation server

For information about gathering installation log files, see the topic about running the information must gather tool. Go to the link at the end of the topic.

Application server

Table 96. 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 |

Table 96. Application server components and log files (continued)

| Component | Log files |
|---|--|
| 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 |
| 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 | <ul style="list-style-type: none"> • /datahome/proxy/idsslapp-tdsproxy/logs/ibmslapd.log |
| WebSphere Operational Decision Management | <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 |

Data server

Table 97. Data server components and log files

| Component | Log files |
|-------------------------|--|
| Tivoli Directory Server | <ul style="list-style-type: none"> • /datahome/dsrdbm01/idsslapp-dsrdbm01/logs/ibmslapd.log • All logs in the /datahome/dsrdbm01/idsslapp-dsrdbm01/logs/ directory |

Event server

Table 98. 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, enter 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 |

Management server

Table 99. 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 | <ul style="list-style-type: none"> • /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log |
| Tivoli Enterprise Portal | <ul style="list-style-type: none"> • /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log |

Table 99. Management server components and log files (continued)

| Component | Log files |
|-------------------------|--|
| 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 |

Related concepts:

“Managing log files” on page 247

IBM Intelligent Operations Center stores log files in several different locations. To prevent system performance issues, periodically archive log files and remove the original log files.

Related tasks:

“Running the installation must gather tool” on page 283

Log files are generated while IBM Intelligent Operations Center is installed. A tool is available to gather these log files for analysis.

Related information:

How to use the System Verification Check tool

The System Verification Check tool is used to determine the operational status of services comprising the IBM Intelligent Operations Center system.

Installing and using IBM Support Assistant Lite

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

ISA Lite gathers the following types of information:

- Platform problem determination files
- System log and trace files
- Platform provisioning files
- System configuration files
- Java™ dump files
- Problem determination framework internal log files

To download ISA Lite for IBM Intelligent Operations Center 1.5, see the link at the end of the topic.

To install and use ISA Lite, follow the instructions in the Quick Start Guide included in the download package.

Related information:

 [Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5](#)

IBM Intelligent Operations Center messages

Each message topic helps you to identify the cause of a particular error condition in the IBM Intelligent Operations Center and recommends actions to take to resolve the error.

To help you understand the errors that you might encounter while using IBM Intelligent Operations Center, each message topic is divided into three sections: the message that is displayed in the IBM Intelligent Operations Center or its logs, an explanation, and an action.

The message

Contains two identifiers, which are the error identification and associated text. The error identification is the message ID. It is a unique number that identifies a message. A final character of E indicates that the message resulted from an error, W indicates a warning message, and I indicates an information message.

The explanation

Contains an additional explanation of the message.

The user response

Suggests the corrective action for resolving the error.

To help you search for information about an error message, enter the ID number of the error message in the Search field in the information center.

Note: The topics in this section contain only messages that are specific to IBM Intelligent Operations Center. For all other messages, see the product documentation.

CIYBA0101E The Topology File {0} is not valid.

Explanation: The installer attempted to validate the {0} topology file and found that the topology file contained errors. These errors can include:

- Not all required components existing in the topology file.
- Prerequisite components not listed before dependant components.
- Components that should be deployed sequentially are in the parallel development stanza.

User response: Correct the topology file and rerun the installation.

CIYBA0102E The topology or the topology specification files were not found.

Explanation: Each installation topology has an associated .xml file and specification. One or both of these files could not be found.

User response: Make sure that all the installation files were extracted to the installation server. Check that the image.basedir.local property in the custom.properties file is set to the correct location. The custom.propeties file is in the /resource subdirectory on the installation server where the installation package was extracted.

CIYBA0103E The {0} script to install a component does not exist.

Explanation: The installation program attempted to locate a script for a component and that script was not found.

User response: Check that the installation media was extracted on the installation server. Check that the base directory was correctly configured in the custom.properties file. The base directory is used to derive the location of the installation script.

CIYBA0104E The Topology file contains invalid entries.

Explanation: The installer encountered an error while reading the topology file and creating the deployable units for each component. This is normally an internal error unless a custom topology is being installed.

The topology file might be corrupted or incorrectly specified.

User response: Check the topology file for the following problems:

- Duplicate component IDs.
- Missing component IDs or type attributes.
- Specification of a connection attribute where no parent component exists.
- The topology fails XML schema validation.

CIYBA0105E The {0} file could not be found.

Explanation: The installation program could not find the {0} file.

User response: Make sure that all the installation files were extracted to the installation server. Check that the image.basedir.local property in the custom.properties file is set to the collect location. The custom.propeties file is in the /resource subdirectory on the installation server where the installation package was extracted.

CIYBA0106E The {0} file could not be saved.

Explanation: The installation program attempted to write the file named {0} and a file I/O error was returned.

User response: Check that the specified location can be accessed using the installer's user ID. Make sure there is sufficient space on the disk and that the partition is not corrupt.

CIYBA0107E Property reference {0} was not found in Topology file {1}

Explanation: During installation some of the components require property values from prerequisite software. These components use properties references in the topology file to determine the required property values. The property reference could not be found in the topology file.

User response: The topology file is corrupted. This could be due to manual edits that introduced invalid entries or that the installation did not write a topology file with correct values. Determine which components were incorrectly installed. Remove any incorrectly installed components, correct the topology file, and reinstall.

CIYBA0108E Component {0} was not found in Topology file {1}.

Explanation: The installation program expected to find the {0} component ID in the {1} topology file. The component ID was not found. The problem might be due to an incorrectly specified dependency in a connection element of another component.

User response: Review the topology file for references to {0}. Correct any incorrect connection elements for the {0} component and reinstall.

CIYBA0109E Property {0}.{1} in Topology File {2} is invalid.

Explanation: The property was not found in the topology file or in a specification properties file.

User response: If missing, add the property to the specification properties file or the topology file. This error might also be due to the property being misspelled. Correct the topology file or specification properties file and reinstall.

CIYBA0110E The property {0}.{1} in Topology File {2} cannot be found.

Explanation: A deployable unit reference another deployable unit indicated by role {1}. Either the dependent deployable unit is not found or there is a mismatch in roles.

User response: The topology file indicated contains references to the property shown, however the definition of that property cannot be found in the topology file. This situation could arise if the topology file was manually edited and a component was removed, however references to that component still exist.

CIYBA0111E Cannot retrieve master host for component {0}.

Explanation: A topology component must be associated with a target host. An orphan topology component is specified.

User response: Check the {0} topology component and make sure it has a sequence of connection attributes that ultimately has a component with a host attribute.

CIYBA0112E Failed to read Topology File {0}

Explanation: The installation program was unable to read the specified topology file.

User response: Check that the indicated topology file is in the installation directory and that the installation program can access the directory.

CIYBA0113E Failed to save file {0}.

Explanation: The installation program was unable to save the indicated file.

User response: Check that the installation program has access to the installation directory.

CIYBA0114E The {0}.{1} property cannot be set.

Explanation: The installation program was unable to update the indicated property.

User response: The topology file is either corrupted or was manually edited and introduced invalid property values. Correct the topology file and rerun the installation.

CIYBA0115E The Topology File {0} cannot be found.

Explanation: The installation program was unable to access the indicated topology file.

User response: Check that the topology file is in the directory specified by the installation program and make sure the installation program can access the directory.

CIYBA0116E Unable to write to properties file {0}.

Explanation: The installation program was unable to write the indicated properties file.

User response: Check that the user ID used by the installation program has access to the temporary directories on the target servers. The directory on the target servers where the temporary installation scripts will be written is specified by the `Unix.script.basedir.remote` property in the `custom.properties` file. Correct this property value if incorrectly specified.

CIYBA0117E The installer failed to create the keystore.

Explanation: The installation program was unable to create the key store.

User response: Check that the user ID being used by the installation program has access to all subdirectories where the installation media was extracted.

CIYBA0118E The installer was unable to access the keystore using the supplied password. The password is incorrect or the keystore is corrupt.

Explanation: The installation program was unable to access the keystore.

User response: Check that the supplied password is correct and the keystore was not corrupted. Regenerate the keystore with a new password by reinstalling the solution.

CIYBA0119E Unable to encrypt property {0} in Topology file {1}.

Explanation: The installation program attempted to encrypt the indicated property using the password supplied in the topology file and was unable to do so.

User response: Check that the keystore is not corrupted and that the password for the topology is correct. If needed, recreate the keystore with a new password by reinstalling.

CIYBA0120E Unable to decrypt property {0} in topology file {1}

Explanation: An attempt to read and decrypt the indicated property failed.

User response: Check that the user ID used by the installation program can access the indicated topology file and that the topology file is in the expected location. Check that the password and secret key are correct. Rerun the installation.

CIYBA0121E The keystore file {0} already exists.

Explanation: This error should not occur using the IBM Installation Manager installation. IBM Installation Manager controls the installation flow and ensure there an attempt is not made to regenerate the keystore.

User response: Check that the installation has not already been run. Rerun the installer once the existing keystore from a previous installation attempt has been removed.

CIYBA0122E The keystore for the Topology does not exist. Run the createSecretKey command.

Explanation: This error should not occur when running the IBM Installation Manager installation. The IBM Installation Manager installation automatically accepts the SecretKey and generates the keystore.

User response: If running a step-by-step installation, follow the steps to generate a keystore.

CIYBA0123E The Topology {0} is not completely installed.

Explanation: The installation program has determined that not all the components in the topology have been installed.

User response: Check the topology file and determine which components have not been installed. Restart the installation.

CIYBA0124E The {0} properties file cannot be found.

Explanation: The installation program attempted to read the indicated properties file. However, the file could not be found.

User response: Check that the installation package was property extracted. Check that the user ID used by the installation program has access to all directories where the package was extracted.

CIYBA0125E Unable to write to the properties file {0}

Explanation: The installation program attempted to update a file with the runtime variable values and an I/O exception was returned.

User response: Check that the location specified can be accessed using the installation program user ID. Check that there is sufficient space in the file system and the disk partition is not corrupt.

CIYBA0126E Unable to set the value for property {0} from Topology file {1}

Explanation: The installation program was unable to set the specified property value.

User response: Check that the property in the indicated topology file has the correct XML syntax. Check that the topology file is not corrupt or malformed. Remove any special characters from the file and restart the installation.

CIYBA0127E Unable to read the solution specification file {0}

Explanation: The installation program tried to read the indicated file and a file I/O error was returned.

User response: Check that the file exists in the specified location. Check that the user ID used by the installation program has access to all directories where the package was extracted.

CIYBA0128E The {0} file could not be saved.

Explanation: The installation program attempted to write the indicated file and a file I/O error was returned.

User response: Check that the location specified can be accessed by the user ID used by the installation program. Check that there is enough space in the file system and that the disk partition is not corrupt.

CIYBA0129E Unable to read the solution package file {0}.

Explanation: The installation program attempted to read the indicated file and a file I/O error was returned.

User response: Check that the file exists in the specified location. Check that the user ID used by the installation program has access to all directories where the package was extracted.

CIYBA0130E The solution package file : {0} does not exist.

Explanation: The installation program tried to read the indicated file and a file I/O error was returned.

User response: Check the permissions of the file indicated in the message. Ensure the user ID used by the installation program has permission to read the file. Modify the file permissions if needed.

CIYBA0131E The installer failed to load the {0} Topology file. File I/O message was {1}.

Explanation: The indicated error was returned when attempting to import the specified topology file.

User response: Check that the indicated topology file is in the correct directory. Check that the topology file does not contain any invalid characters. Check that the installation program can access the directory containing the topology file.

CIYBA0140E Unable to access required installation files.

Explanation: The installation program attempted to read a required file and was unable to do so.

User response: Check that the location where the installation package was extracted can be accessed by the user ID used by the installation program. Make sure the disk partition is not corrupt. Extract the installation package again and retry the installation.

CIYBA0141E Unable to locate installation file {0}.

Explanation: The installation program attempted to read the indicated file and a file I/O error was returned.

User response: Check that the file exists in the specified location. Check that the user ID used by the installation program can access all directories containing the extracted installation package.

CIYBA0142E Unable to write to installation file {0}.

Explanation: The installation program tried to write the indicated file and a file I/O error was returned.

User response: Check that the user ID used by the installation program has access to all directories containing the extracted installation package. Check that the disk partition is not corrupt and has not run out of space.

CIYBA0143E The installation program failed to process the Topology File.

Explanation: The installation program reads the topology file and generates intermediate files containing runtime values. The installation program encountered an error while processing the topology file and writing the intermediate files. File I/O errors are the likely cause of this error.

User response: Check that the user ID used by the installation program has access to all directories where the installation package was extracted. Check that the disk partition is not corrupt or out of space.

CIYBA0150E Unable to read the Topology Specification file {0}.

Explanation: The installation program tried to read the indicated file and a file I/O was returned.

User response: Check that the file exists in the specified location. Check that the user ID being used by the installation program has access to all directories where the installation package was extracted.

CIYBA0160E The rule specification file was not found in the {0} directory.

Explanation: The installation program tried to load the rule-spec.xml file, which defines the precheck rules, and was unable to do so.

User response: Check that the indicated directory exists. Also make sure the directory can be accessed by the user ID used by the installation program.

CIYBA0161E The rule name {0} is invalid.

Explanation: The installation program identified an incorrect rule name in the rule-spec.xml file. This file defines rules used by the precheck step.

User response: Check that the rule name is correct in the rule-spec.xml file. Refer to an unchanged version of the rule-spec.xml file for the correct rule name.

CIYBA0162E Installation prerequisite checking failed for topology {0}.

Explanation: The precheck step has failed with one or more of the configuration targets failing to meet the supported system requirements.

User response: Check that the planned topology meets the minimum supported requirements.

CIYBA0163W The OS type of target server {0} is not {1}.

Explanation: The precheck step has detected an unsupported operating system on the indicated target server.

User response: Make sure the operating system on the target server meets the supported system requirements.

CIYBA0164W The {0} server was expected to have a {1} bit OS.

Explanation: The precheck step has detected an incorrect operating system on the target server.

User response: Check that the operating system type on the target server meets the system requirements.

CIYBA0165W CPU of target server {0} is not a x86 or s390 64bit CPU.

Explanation: The precheck step has detected an unsupported CPU type for the indicated target server.

User response: Check that the CPU type for the target server meets system requirements.

CIYBA0166E Cannot connect to target server {0}.

Explanation: The installation program could not connect to the remote server when running the precheck step.

User response: Check connectivity between the installation server and the target servers. Check the precheck logs for other errors.

CIYBA0167E Cannot connect to server {0} because of the wrong host name, account or password was specified.

Explanation: The installation program failed when running the precheck step. The installation program was unable to connect to the target server.

User response: Check that the hostname is the correct format and the login details are correct for the remote server. Check the precheck logs for additional information.

CIYBA0168E The time or timezone for servers {0} and {0} are not synchronized.

Explanation: There is a difference between time or time zones set for the servers.

User response: Check that the time and time zone is the same for all servers.

CIYBA0169W Check OS type and CPU architecture on server {0}

Explanation: The installation program precheck step has found an unsupported operating system and CPU architecture for a target server.

User response: Make sure all servers meet the system requirements for the solution.

CIYBA0170W Check time zone and date & time on all servers

Explanation: This message is followed by the word "pass" or "fail". What follows determines the action to be taken.

User response: If the message is followed by "pass", no response is required. If the message is followed by "fail", then the servers must be synchronized. The time zone, date and time system parameters must be the same for each node in the topology.

CIYBA0171I Installation prerequisite checking is starting using instance {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0172I Installation prerequisite check finished successfully.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0173I Installation prerequisite check finished with {0} warnings and {1} errors:

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0176E The login information for server {0} is incorrect. Verify the user id and password for the server.

Explanation: The installation program precheck step found incorrect login information for the target server.

User response: Check that the account details for the server have the correct user ID and password.

CIYBA0177W Unable to connect to the remote server. Waiting to retry.

Explanation: The installation program precheck step failed to connect to the remote server. The connection will be reattempted.

User response: No action is required. The installation program will wait the amount of time specified in the `waiting.time` property in the `custom.properties` file and will then reattempt the connection.

CIYBA0178W Cannot connect to {0}, waiting {1} milliseconds before next connection attempt.

Explanation: There are connectivity issues in the system.

User response: If multiple connection attempts fail, contact the network administrator to resolve the connectivity issues and retry the installation.

CIYBA0179E No value was provided for key {0} in the topology properties file.

Explanation: The installation program precheck step was unable to retrieve values for the hostname, user name, or password from the properties file.

User response: Check that the hostname, user name, and password are specified correctly in the properties file.

CIYBA0180E The user id entered for server {0} does not have root privileges.

Explanation: The installation program precheck step detected that the account used for the indicated server does not have root privileges.

User response: Change the user ID used for the server to one that has root privileges or add root privileges to the user ID specified for the server.

CIYBA0181E Verify the root user id and password for server {0}.

Explanation: The installation program precheck step determined that the user ID used for the server has insufficient access rights.

User response: Check that the account has sufficient access rights.

CIYBA0182E Check connectivity from install server to {0}

Explanation: The installation program precheck step failed to connect between the installation server and the target server.

User response: Check the connectivity between servers. Review the precheck logs for additional information.

CIYBA0183E Value {0} for key {1} in not valid, it should be "EM64T" or "AMD64" or "S390".

Explanation: The key value should be one of the specified values.

User response: Correct the value and rerun the installation.

CIYBA0184E Value {0} for key {1} is not a valid host name

Explanation: The installation program precheck step determined the value provided is not a valid hostname.

User response: Check that the host name is the correct format and has a correct value.

CIYBA0185E Install prerequisite check failed on rule {0}

Explanation: The installation program precheck step failed when checking the specified rule.

User response: Check the precheck logs for addition messages. Correct the error and retry the installation.

CIYBA0187E SSH keystore "{0}" was specified, but could not be accessed. Certificate-based SSH protocol will be unavailable. Details: {1}.

Explanation: The installation program precheck step detected invalid data in the SSH keystore when attempting to connect to the target server.

User response: Review the details in the message and verify that the provided keystore has adequate entries.

CIYBA0190E The component {0} must appear before component {1} in topology file.

Explanation: The topology file was incorrectly changed. A prerequisite component appears after a component that depends upon it.

User response: Change the topology file so the components that have dependencies are after the components they depend on.

CIYBA0191E There is a dependency between component {0} and component {1} in the Topology File. The components cannot be deployed in parallel.

Explanation: The components cannot be deployed in parallel if there is a dependency between them. For example, if component 2 is a prerequisite of component 1.

User response: Remove the components from the parallel stanza of the topology file.

CIYBA0192E The property {1}.{2} has an invalid reference value of {0} in the Topology File.

Explanation: The reference value included in the message is not valid for the indicated property.

User response: Use the ID field to find the property definition and make sure all references to the property have the correct value.

CIYBA0193E The component {0} has duplicate connections {1} identified in the Topology File.

Explanation: Duplicate connections for the component are defined in the topology file.

User response: Remove the duplicate connection information in the topology file and rerun the installation program.

CIYBA0194E The property {0} is duplicated in component {0}

Explanation: A duplicate property is defined for the component.

User response: Remove the duplicate property for the component in the property file.

CIYBA0195E The component {0} in the Topology file has an invalid property {0}.

Explanation: The property specified was unexpected for the indicated component. This could be caused by a misspelled property or a property missing from the property specification.

User response: Add the specified property to the properties file or the topology. If the property was misspelled, correct the misspelling. Correct the topology file or specification properties file and restart the installation.

CIYBA0196E The component {1} is missing property {0}

Explanation: The component must have the indicated property. The error could be caused by a misspelled property or due to the property being missing from the property specification file.

User response: Add the property to the specification properties file or topology. If the error is due to a misspelling, correct the misspelling. Restart the installation.

CIYBA0197E Component {1} has an invalid component type {1} specified.

Explanation: An invalid component type was specified for the component.

User response: Check that the specification file for the component contains the component type. Component specification files are located in the *install_home/spec/component* subdirectory on the installation server.

CIYBA0198E The connection {0} is not valid for component {1}

Explanation: The defined connection is not valid for the component.

User response: Check the spelling of the connection in the topology file for the component and make sure it is not misspelled.

CIYBA0199E The {0} connection was missing from component {1}.

Explanation: No connection is defined for the indicated component.

User response: Check the component specification file and make sure the connection information is included.

CIYBA0200E The connection information for {0} does not exist.

Explanation: The connection ID is missing for the indicated component.

User response: Check that the connection ID is specified in the topology file. Check that the connection ID is spelled correctly and refers to a stanza in the topology file defining the associated component for the connection ID.

CIYBA0201E Can not connect to remote server {0}.

Explanation: The installation program found a connectivity problem to the indicated server.

User response: Check that there are no connection issues between the servers. Run the installation program precheck step and resolve any connectivity issues.

CIYBA0202E User name or password is invalid for server {0}.

Explanation: The installation program found invalid credentials for the indicated server.

User response: Check that the server credentials are correct in the topology file.

CIYBA0203E File {0} does not exist.

Explanation: An attempt to load the properties file returned an error.

User response: Check that the path to the properties file is correct and that the file exists.

CIYBA0204E Can not read/write file {0}.

Explanation: The installation program tried to load the properties file and an error was returned.

User response: Check that the properties file path is correct and the indicated file exists.

CIYBA0205E Can not create directory {0} on {1}.

Explanation: The installation program was unable to create a directory on the remote server.

User response: Check that there is enough space on the remote server and that the user ID used by the installation program has sufficient access rights and adequate permissions to create a directory.

CIYBA0206E Fail to upload file {0} to remote directory {1} on server {2}.

Explanation: The installation program was unable to copy files to the indicated directory on the remote server.

User response: Check that there is enough space on the remote server and that the user ID used by the installation program has sufficient access rights and adequate permission to write files to the remote server.

CIYBA0207E No image defined for {0}.

Explanation: The installation program was unable to retrieve image data for the properties file.

User response: Check that the properties file contains an image field with the data component.

CIYBA0208E Fail to upload image of component {0} to remote server {1}.

Explanation: The installation program was unable to copy the image files to a directory on the remote server.

User response: Check that there is enough space on the remote server and that the user ID used by the installation program has sufficient access rights and adequate permission to write to the directory on the remote server. Also check that the remote directory name is correct.

CIYBA0209I Host name : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0210I OSType={0},OSBit={1},CPUArch={2}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0211I Remote path : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0212I Local path : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0213E Fail to download file {0} from remote server {1}.

Explanation: The installation program was unable to copy the image files from a remote directory server to the local server.

User response: Check that there is enough space on the local server and that the user ID used by the installation program has sufficient access rights and adequate permissions to write to the directory. Also check that the local and remote directory names are correct.

CIYBA0214E Download file {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0215I Command : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0216I Command exit code : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0217I Command output : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0218E Command failed with return code {0}.

Explanation: The command did not successfully complete.

User response: Check the log files for further details.

CIYBA0219I Upload file {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0220I Local image dir : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0221I Remote image dir : {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0222E Remote image {0} already exists.

Explanation: The file already exists on the target server. The installation process includes transferring media to target servers. This message indicates the required image has already been transferred.

User response: This message indicates that media from a previous installation attempt still exists on the target servers. If the user intended to start a new installation, the media should be deleted so that it can be uploaded again.

CIYBA0223E Can not launch command on server {0}.

Explanation: The installation program could not run the **IOC** command from the remote server to the local server.

User response: Check the connection between the local server and the remote server. Check that the user ID used by the installation program has sufficient access rights and adequate permission to run the command.

CIYBA0224E Get backup files from folder {0} on server {1}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0225E Fail to Get backup files from folder {0} on server {1}.

Explanation: The installation program was unable to retrieve files from a remote backup folder to a local folder.

User response: Check the connection between the local and remote servers. Check that the user ID used by the installation program has sufficient access rights and adequate permission to access the folders.

CIYBA0226E No backup folder {0} exists on server {1}.

Explanation: The installation program was unable to retrieve files from a remote backup folder to a local folder.

User response: Check that the remote directory and folder exists.

CIYBA0227E Value must be provided for id and path attribute.

Explanation: The installation was unable to identify the component ID and path attribute.

User response: Check that the component ID and path arguments are provided within the task arguments.

CIYBA0228I Exec command: {0}.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0229E Insufficient disk space in target directory {0}.

Explanation: The installation program did not find enough space in the target directory.

User response: Check that the indicated directory has

enough allocated space and can be accessed by the user ID used by the installation program.

CIYBA0230I IOC Command Line Version: {0}

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0231I Import topology "{0}" successfully

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0232E Topology name "{0}" is not found under ../topology folder

Explanation: The installation program was unable to find the indicated topology in the ../topology folder.

User response: Check that the topology file exists in the ../topology folder and that it is in a valid XML format.

CIYBA0233I Current topology is "{0}".

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0234E ANT_HOME is not set or set incorrectly. Please set ANT_HOME.

Explanation: The installation program encountered a problem in the ANT_HOME environment variable.

User response: Check that the ANT_HOME variable is set to a valid ANT version.

CIYBA0237E Component ID "{0}" is invalid.

Explanation: The installation program found an incorrect component ID in the topology file.

User response: Check that the component ID exists and is named correctly in the topology file.

CIYBA0238E Action "{0}" for component ID "{1}" is invalid.

Explanation: The indicated action is incorrect for the current component in the topology file.

User response: Check the topology file and make sure the defined action is suitable for the component.

CIYBA0239E If you want more detailed operation messages, please check {0}.

Explanation: The command did not successfully complete.

User response: Check the log file indicated by {0} for actions to be taken.

CIYBA0240I Command finished successfully.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0241E Command failed :

Explanation: The displayed command failed.

User response: The action to be taken will depend on the command that failed. Review the command and the logs to determine the cause of the failure.

CIYBA0242E Please remove the ".xml" from parameter "{0}".

Explanation: The parameter shown includes the file extension .xml.

User response: XML filename parameters should not include the .xml extension. Remove .xml from the parameter and retry the command.

CIYBA0243E IOP_CIPHER_ALG or IOP_CIPHER_KEYSIZE environment variables incorrectly set. Please set to appropriate JCE-compliant values."

Explanation: The installation program was unable to identify a correct value for the cipher used in the encryption.

User response: Check that the CIPHER_ALG and IOP_CIPHER_KEYSIZE environment values are correctly set.

CIYBA0244E "{0}" is not a valid parameter.

Explanation: The indicated parameter is not a valid parameter.

User response: Remove or correct the parameter and retry the command.

CIYBA0245E "-{0}" miss parameter.

Explanation: The indicated parameter is required but missing from the command.

User response: Rerun the command with the missing parameter.

CIYBA0249I Prepare operation scripts.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0250I Operation complete.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0251I Operation sequence started.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0252I Operation sequence finished.

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0253I Upload component [{0}] images to host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0254I Install component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0255I Uninstall component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0256I Start component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0257I Stop component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0258I Propagate component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0259I OK

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0261I {0} task(s) are running

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0262I The total {0} task(s) will be performed

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0263I Backup component [{0}] on host [{1}]

Explanation: This message is for informational purposes only.

User response: No action is required.

CIYBA0264E Can not load log configuration file {0}.

Explanation: The logging function cannot find the property file containing the logging configuration parameters.

User response: Check that installation package was fully extracted and that it is located on a file system accessible to the user ID running the installation program.

CIYBA0265E Can not create file handler for log.

Explanation: The logging function attempted to open a file using a system file handle and was unable to do so.

User response: Have the system administrator check the number of file handles available to the system. Ensure the file system where the installation package was extracted is not corrupt.

CIYBA0266E The required RPM package {0} is not installed on the {1} server.

Explanation: The indicated RPM package is not installed on the server.

User response: Install the supported RPM package on the server.

CIYBA0267E The {1} server does not have enough disk space. {0} disk space is required.

Explanation: The server does not have enough disk space or the server does not meet the system requirements for disk space.

User response: Delete files to make space available on the server so the minimum space requirements are met.

CIYBA0268E The {1} server does not have enough memory. {0} GB of memory is required.

Explanation: There is not enough RAM on the indicated server. The server does not meet system requirements for minimum RAM.

User response: Add RAM to the server.

CIYBA0269E The {0} directory can not be created on server {1}. The directory already exists.

Explanation: The specified directory already exists on the server.

User response: Remove the directory on the server.

CIYBA0270E The tcp ip port {0} is in already in use on server {1}. This is a required port and must be available prior to installation.

Explanation: The program or process is already configured to use a required TCP/IP port on the server.

User response: Reconfigure the server so the required port is available. Rerun the installation.

CIYBA0271E Server {1} does not have the expected Fully Qualified Host Name. The expected FQH is {0}.

Explanation: The server does not have the expected fully qualified host name.

User response: If using the IBM Installation Manager installation, enter the fully qualified hostname for the server. If using the step-by-step installation, enter the fully qualified host name in the SERVERS section of the topology Properties file. Correct the server listed in the error message.

CIYBA0272E The network connection from server {1} to server {0} is broken.

Explanation: There is no network connectivity between the two indicated servers.

User response: Check the connectivity between the servers. If the problem persists, contact the system network administrator.

CIYBA0273E Server {0} is running SELinux which is unsupported.

Explanation: SELinux is not supported by IBM Intelligent Operations Center.

User response: Install a supported Linux version.

CIYBA0274E An active firewall was detected on server {0}. All firewalls must be disabled prior to installation.

Explanation: The server has an active firewall.

User response: Disable the firewall on the server during the installation process.

CIYBA0275E Unable to find a DNS entry for server {0}. DNS lookup by IP or Host Name failed.

Explanation: The server is either not configured correctly in the DNS, or the DNS is not functioning properly. The DNS lookup command failed for the server by IP address and by host name.

User response: Contact the system network administrator for the server and correct the DNS entry of DNS

CIYBA0276E Server {1} has a system setting that does not meet installation requirements. The maximum number of open files [unlimit] is less than {0}.

Explanation: The system setting for the maximum number of open files does not meet installation requirements.

User response: The `ulimit` setting needs to be modified to the indicated value.

CIYBA0277E The Linux request found does not meet installation requirements. The expected release is {0}.

Explanation: The Linux installed on the indicated server is not supported.

User response: Install a supported Linux version.

CIYBA0278E The Linux distribution found does not meet requirements. The expected distribution is {0}

Explanation: The Linux installed is not supported.

User response: Install a supported Linux distribution.

CIYBA0279E WebSphere Application Server profile {0} is not started or account or password is invalid on server {4}.

Explanation: The WebSphere Application Server profile is not started or an attempt was made to start it with invalid credentials.

User response: Start the WebSphere Application Server profile using a correct user ID and password.

CIYBA0281E Server {0} does not have IPv6 enabled. Enable IPv6 on the server before installation.

Explanation: The indicated server does not have IPv6 configured.

User response: Enable IPv6 on the indicated server.

CIYBA0282E Some of the files located in the {0} directory on the media server are corrupt.

Explanation: All installation files have MD5 checksums that need to be verified prior to installation. The MD5 checksum on some files located in the indicated directory do not have valid MD5 checksums.

User response: Extract the installation package again, or recopy the files to the directory.

CIYBA0283E SSH on server {0} is not configured correctly. Password authentication using SSH is needed but not configured on server.

Explanation: The SSH configuration on the indicated server is incorrect.

User response: Reconfigure the /etc/ssh/sshd_config file as follows:

- Remove all AllowUsers statements.
- Specify YES for PermitRootLogin.
- Specify YES for Password Authentication.

These changes will allow only root users to access the server using SSH with password authentication.

CIYBA0284E {0} was found to be a symbolic [soft] link. Symbolic links are not permitted.

Explanation: Symbolic or soft links to files or directories are not supported.

User response: Remove symbolic links and provide the direct path or file name.

CIYBA0285E Tivoli Directory Server instance {0} is not started on server {1}.

Explanation: The indicated Tivoli Directory Server instance needs to be started.

User response: Start the Tivoli Directory Server.

CIYBA0286E IBM DB2 instance {0} is not started on server {1}.

Explanation: The indicated DB2 instance is not started.

User response: Start the DB2 instance.

CIYBA0287E WebSphere Application Server {1} on profile {0} is not started on server {2}.

Explanation: The indicated WebSphere Application Server profile is not started on the indicated server.

User response: Start the WebSphere Application Server profile.

CIYBA0288E Server {0} does not have "localhost" mapped to 127.0.0.1.

Explanation: In the host file for each server the localhost entry must be mapped to 127.0.0.1.

User response: Update the host file on the server to map the localhost value to 127.0.0.1.

CIYBA0289E Server {0} does not have enough CPU Resource. CPU Resource count on server is {1}

Explanation: The server does not have enough CPU resources to meet requirements.

User response: Add CPU resources to the indicated server.

CIYBA0301E A button was clicked to run a test but no matching properties were found in the properties file.

Explanation: The properties for the test were not found in the properties file.

User response: Click Reset. This will cause the program to read the current properties file in case changes were made. Retry the test.

CIYBA0302E Every test must have certain properties. class is one of them. Parameters: {0}; class name {1}; method name {2}; sequence number

Explanation: Test definition is missing the class property.

User response: Search for the sequence number in the

properties file. Add a class property for the test. This is the class name of the test. This is usually the class name of the remote execution agent (the code that forwards the test request to IopCatRemoteResponder for execution.

For example:

```
0070.className=com.ibm.iop.cat.fw.remote.IopCatRemoter
```

CIYBA0303E Every test must have certain properties. display label is one of them. Parameters: {0}: class name {1}: method name {2}: sequence number

Explanation: Test definition is missing the display label.

User response: Search for the sequence number in the properties file. Add a `displaylabel` property for the test. This is the text that will be displayed on the button.

CIYBA0304E A button was clicked to run a test but no matching test was found in the properties file.

Explanation: The currently loaded properties file does not define the requested test.

User response: Click **Reset**. The current properties file will be reloaded.

CIYBA0305E A button was pressed to run a test but no configuration information can be found for the test.

Explanation: Configuration information is not available for the test.

User response: Click **Reset**. The current properties file will be reloaded.

CIYBA0306E The code specified by the class could not be found. Parameter:{0}: class name (not found)

Explanation: Either the `classname` was not specified correctly in the properties file or the code was not found.

User response: Check the shared libraries for the IopCatRemoteResponder application to see if one or more shared libraries are missing or not specified.

CIYBA0307E Common variables apply to all tests. It is not allowed to set the name, class or debug using common. Parameters: {0}: class name {1}: method name {2}: property key string

Explanation: Common was used to set name, class, or debug.

User response: Search for the key and remove the offending line. For example, `common.name` used to name all tests with the same name.

CIYBA0308E An exception occurred in class {0}, method {1}. Details {2}

Explanation: An exception occurred.

User response: Examine the exception string to determine why the test failed. This may be a normal test failure. For example, "Connection refused" usually means no program was listening on a given port so the service is not running.

CIYBA0309E {0},{1}() - Test[{2}] - Exception: {3}

Explanation: A runtime exception occurred in the indicated test.

User response: Review the error message for details.

CIYBA0310E An unexpected Exception occurred while running this test.

Explanation: An unexpected exception occurred.

User response: Review other exceptions for additional details.

CIYBA0311I The string returned from the internal diagnostic echo test. Parameter {0}: input properties to the test.

Explanation: Displays the input properties for the test.

User response: This is a normal message and not an indication of an error.

CIYBA0312E The Web test received the expected HTTP response code (either in the 200's or specified by the property expectedRcode). Parameters: {0}: class name

Explanation: Indicates the test was successful.

User response: No action is required.

CIYBA0313E The Web test did not receive the expected HTTP response code (either in the 200's or specified by the property expectedRcode). Parameters: {0}: class name {1}: HTTP response code

Explanation: An unexpected HTTP response code was received.

User response: Check the URL specified by the `hosturl` property either with a browser or the `wget` command.

CIYBA0314E The string representation of the test response. Parameters: {0}: response code {1}: response text {2}: additional test specific text

Explanation: This message returns the test response as a string.

User response: No action is required.

CIYBA0315E All tests must have properties. No properties were passed into this test.

Explanation: Properties were missing from the test invocation.

User response: This message should not occur since properties are passed by the framework. Contact IBM Software Support.

CIYBA0320E An expected string was not found in the text properties. Class name {0}, output text {1}

Explanation: The SSH tests login to the server, runs the commands, and checks for an expected string in the output from the commands. No expected string was specified in the properties for this test.

User response: Check the expected key for the test. Add or modify the property to specify a string expected to be contained in the output for the commands specified in the commands property.

CIYBA0322E Expected string not found in output. Class name {0}, output text {1}

Explanation: The SSH tests log on to the server, runs the commands, and checks for an expected string in the output from the commands. The expected string was not found in the output.

User response: Check the expected key for the test and the output text. This could indicate the test failed. If the output text contains "keyboard interactive not allowed" it could mean that the user ID or password used to log on to the remote server is incorrect. Check the user, password, and hostname properties for the test. The password is an alias to a password in the keystore.

CIYBA0323E Unexpected exception in class name {0}. Exception: {1}

Explanation: An unexpected exception occurred.

User response: If the output text contains "keyboard interactive not allowed" it could mean that the user ID or password used to log on to the remote server is incorrect. Check the user, password, and hostname properties for the test. The password is an alias to a password in the keystore.

CIYBA0340E The test execution agent (IopCatRemoteResponder) was unable to parse the input JSON data. Parameters: {0}: class name {1}: method name {2}: post data

Explanation: The user interface and test execution agent communicate using JSON. This error means the test execution agent (IopCatRemoteResponder) was unable to parse the input JSON data.

User response: Examine the post data to see if it is in the correct JSON format.

CIYBA0341E An exception was encountered while running the test. Parameters: {0}: class name {1}: method name {2}: exception string

Explanation: An exception was encountered while running the test.

User response: Check the exception string to determine why the test failed. This might be a normal test failure. For example, "Connection refused" usually means no program was listening on the port so the service is not running.

CIYBA0342E The test execution agent (IopCatRemoteResponder) was unable to send a reply back to the user interface. Parameters: {0}: class name {1}: method name {2}: exception string

Explanation: The user interface and test execution agent communicate using JSON. This error means the test execution agent (IopCatRemoteResponder) was unable to send a reply back to the user interface.

User response: Check the exception string to determine why the reply could not be sent. This could occur if the test took too long and the user interface is no longer waiting.

CIYBA0343E An expected Key prefix is missing. Parameters: {0}: class name {1}: method name {2}: property key string

Explanation: All properties for a given test are prefixed by the same number. This provides the grouping since properties files are not positional.

User response: Search for the key in the properties file and add the appropriate prefix. For example, the following is incorrect:

```
classname      - com.ibm.iop.cat.fw.remote.IopCatRemoter
0950.rhosturl  - https://$[APP_HOSTNAME_1]:9443/IopCatRemoteResponder/IopCatRemoteResponder
0950.remoteclassname- com.ibm.iop.cat.fw.Echo
0950.displaylabel - Internal Diagnostic (Echo REST remoted)
0950.comment    - Self diagnostic CAT check. Tests link between to CAT modules.
0950.fullinfopage - cct_echo_rest_remoted_test.html
```

Should be:

```
0950.classname  - com.ibm.iop.cat.fw.remote.IopCatRemoter
0950.rhosturl  - https://$[APP_HOSTNAME_1]:9443/IopCatRemoteResponder/IopCatRemoteResponder
0950.remoteclassname- com.ibm.iop.cat.fw.Echo
0950.displaylabel - Internal Diagnostic (Echo REST remoted)
0950.comment    - Self diagnostic CAT check. Tests link between to CAT modules.
0950.fullinfopage - cct_echo_rest_remoted_test.html
```

CIYBA0345E Invalid Key - The key prefix is not numeric. Parameters: {0}: class name {1}: method name {2}: sequence number CCT_RESULTS_INFO = {0}.{1}() - Class: {2} Results - Response Code{3}] Response Text{4}]

Explanation: Every test must have a numeric prefix grouping all of the properties for a given test. The prefix given is not numeric.

User response: Search for the sequence number in the properties file. Change the prefix to be numeric and use that same prefix for the rest of the properties for the test.

CIYBA0347E An Exception has occurred. Parameters: {0}: class name {1}: method name {2}: exception string

Explanation: An exception has occurred.

User response: Examine the exception string to determine why the test failed. This might be a normal test failure. For example, "Connection refused" usually means no program was listening on the port so the service is not running.

CIYBA0348E A button was clicked to run a test but no matching properties were found in the properties file.

Explanation: No properties were found for the test. The properties file might have been changed.

User response: Click **Reset**. The current properties file will be reloaded.

CIYBA0349E The code specified by the class could not be found. Parameter: {0}: class name (not found)

Explanation: Either the classname is not correctly specified in the properties file or the code was not found.

User response: Check the shared libraries for the IopCatRemoteResponder to see if one or more shared libraries are missing.

CIYBA0401E The IOPMGMT properties template file name was not specified or was incorrect.

Explanation: The parameter for the IOPMGMT properties template file is missing.

User response: Enter the correct name for the IOPMGMT properties file.

CIYBA0402E The Topology Properties file name was not specified or was incorrect.

Explanation: The parameter for the topology properties file is missing or incorrect.

User response: Enter the correct name for the topology properties file.

CIYBA0403E The IOPMGMT properties template file name was not specified or was incorrect.

Explanation: The parameter specifying the IOPMGMT properties template file is missing.

User response: Enter the correct file name for the topology properties file.

CIYBA0404E The Topology properties file cannot be found.

Explanation: The topology properties file cannot be found.

User response: Check that the topology properties file is located in the *install_home/topology* directory on the installation server.

CIYBA0405E Missing password in the Topology File for property:

Explanation: A password was not found in the indicated topology properties file.

User response: A password for the topology file is required. Enter a password for the topology.

CIYBA0501E The required parameter for the Base Architecture Cyber Hygiene Media is missing.

Explanation: The required parameter for the IBM Intelligent Operations Center cyber hygiene media is missing.

User response: Check that the cyber hygiene script has the correct path to the location of the installation media.

CIYBA0502E The required parameter for the Topology properties file is missing.

Explanation: The file name parameter for the topology properties file is missing.

User response: Supply the correct file name for the topology properties file.

CIYBA0503E The required parameter for the Base Architecture Cyber Hygiene destination directory is missing.

Explanation: The required parameter for the cyber hygiene destination directory is missing.

User response: Supply the correct destination directory.

CIYCC0002E Correct the following configuration errors: {0}

Explanation: There is an error on the Edit Shared Sessions configuration page. The error is indicated by {0}.

User response: Correct the error and retry the request.

CIYCC0005E The event cannot be submitted. Try to submit the event again. If the problem persists, contact an administrator or help desk.

Explanation: A publisher servlet error occurred when a user tried to update, escalate, or cancel an event.

User response: Have the administrator or help desk resolve the publisher servlet error.

CIYCC0006W The record has been updated by another user. Please refresh the page to fetch the updated record.

Explanation: An update requested by the user is conflicting with another change that has occurred on the server. This can happen if two users try to change the state of an activity at the same time.

User response: Refresh the page. The update made by the other user will be displayed. Then make any changes required.

CIYUI0001E The provided JSON array contains errors and cannot be parsed.

Explanation: The user entered a JSON string in a window where the script is to be entered, but the string has syntax errors and cannot be parsed.

User response: Correct the JSON string.

CIYUI0002E Event not found. The event's properties cannot be displayed.

Explanation: The request to display the event's properties failed because the properties were not found in the database.

User response: Refresh the page and retry the request.

CIYUI0004E Location map manager data submission error.

Explanation: A problem occurred while setting the location map manager data.

User response: See additional messages for more details.

Additional messages from the Classifications tab.

Data Submission Error

The new classification has not been entered in the database.

Additional messages from the Location Maps tab.

Data Submission Error

The new location map has not been entered in the database.

Additional messages from the Areas tab.

The area identifier entered is not valid. The area identifier already exists on the map.

The user is entering an area on the map that already exists on the map.

The area identifier entered is not valid.

The area identifier is not valid. Either it is blank or the area ID is equal to the parent area ID.

The area data entered is not valid.

The area data is not valid. The customer should check that they have entered all required fields for each area.

The parent area identifier must not exist as an area on the current map.

The parent area ID entered exists as an area on the map. An area cannot have a parent area which is an area on the map. It must be on another map.

There are circular references between areas and their parent areas. Please remove the circular references.

Remove circular parent area relationships from the IBM Intelligent Operations Center database.

Data submission error.

The new areas tab has not been entered in the database.

CIYUI0003I Data submitted successfully.

Explanation: This message is for informational purposes only. The message indicates that the IBM Intelligent Operations Center database, Location Map Manager portlet, and the Location Map portlet have been updated.

User response: No action is required.

CIYUI0004I Submitted successfully.

Explanation: This message is for informational purposes only. The message indicates that only the Location Map Manager portlet UI is updated, changes are not stored in the IBM Intelligent Operations Center database. If you leave the Location Map Manager

portlet without submitting changes, the update is canceled.

User response: Click **Submit** to update the IBM Intelligent Operations Center database and the Location Map portlet.

Using Knowledge bases and IBM Support

This section contains topics for using Knowledge bases, Fix Central, and IBM Support to find troubleshooting information.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for IBM Intelligent Operations Center, but sometimes you need to look beyond the information center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant Lite (ISA Lite).
ISA Lite is a no-charge software tool that helps you answer questions and resolve problems with IBM software products. For instructions for downloading and installing ISA Lite, see the links at the end of the topic.
- Find the content that you need by using the IBM Support Portal.
The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content about IBM Intelligent Operations Center by using one of the following additional technical resources:
 - IBM Intelligent Operations Center technotes and APARs (problem reports)
 - IBM Intelligent Operations Center Support Portal page
 - IBM Intelligent Operations Center Forums and communities page
 - IBM Smarter Cities Software Solutions Redbooks®
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any [ibm.com](https://www.ibm.com)® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the [ibm.com](https://www.ibm.com) domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on [ibm.com](https://www.ibm.com).

Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

Related concepts:

“About” on page 185

Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation.

“Installing and using IBM Support Assistant Lite” on page 287

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

Related information:

 [Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5](#)

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are recommended by IBM Support for various products, including IBM Intelligent Operations Center. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An IBM Intelligent Operations Center product fix might be available to resolve your problem.

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Intelligent Operations Center as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
 - a. Open the download document and follow the link in the “Download Package” section.
 - b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. To apply the fix, follow the instructions in the “Installation Instructions” section of the download document.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

Related tasks:

“Subscribing to support updates” on page 307

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

Related information:

 [Fix Central help](#)

Contacting IBM Support

IBM Support provides assistance with product defects, answering FAQs, and performing rediscovery.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For

information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

Procedure

Complete the following steps to contact IBM Support with a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information. For information on using IBM Support Assistant Lite to collect IBM Intelligent Operations Center log files, see the links at the end of the topic.
3. Submit the problem to IBM Support in one of the following ways:
 - Using IBM Support Assistant Lite (ISA Lite). See the links at the end of the topic.
 - Online through the IBM Intelligent Operations Center Support Portal page: You can open, update, and view all your Service Requests from the Service Request portlet on the Service Request page.
 - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

What to do next

Be prepared to work with the IBM technical-support representative by using IBM Assist On-Site, which is a remote-assistance plug-in that you can download to your computer. The IBM technical-support representative can use IBM Assist On-Site to view your desktop and share control of your mouse and keyboard. This tool can shorten the time that it takes to identify the problem, collect the necessary data, and solve the problem. For more information, see IBM Assist On-Site.

Related concepts:

“About” on page 185

Use the About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you installed. You can also view details of any updates you applied since installation.

“Installing and using IBM Support Assistant Lite” on page 287

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

Related information:



Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5

Subscribing to support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds

The following RSS feed is available for IBM Intelligent Operations Center: *IBM Intelligent Operations Center*.

For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past.) With My Notifications, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. To subscribe to the *IBM Intelligent Operations Center* RSS feed, use the following substeps:
 - a. Open the link *IBM Intelligent Operations Center* RSS feed.
 - b. In the Subscribe with Live Bookmark window, select a folder in which to save the RSS feed bookmark and click **Subscribe**.

For more information on subscribing to RSS feeds, see the IBM Software Support RSS feeds link in the Related information section at the end of the topic.

2. To subscribe to My Notifications, go to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
3. Sign in using your IBM ID and password, and click **Submit**.
4. Identify what and how you want to receive updates.
 - a. Click the **Subscribe** tab.
 - b. Select *IBM Intelligent Operations Center* and click **Continue**.
 - c. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
 - d. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
 - e. Click **Submit**.

Results

Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Related tasks:

“Getting fixes from Fix Central” on page 306

You can use Fix Central to find the fixes that are recommended by IBM Support for various products, including *IBM Intelligent Operations Center*. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An *IBM Intelligent Operations Center* product fix might be available to resolve your problem.

Related information



IBM Software Support RSS feeds



Subscribe to My Notifications support content updates

 [My notifications for IBM technical support](#)

 [My notifications for IBM technical support overview](#)

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Related concepts:

“Enabling traces and viewing log files” on page 279

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics give some guidance on how to access log files.

“Installing and using IBM Support Assistant Lite” on page 287

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

Related tasks:

“Running the installation must gather tool” on page 283

Log files are generated while IBM Intelligent Operations Center is installed. A tool is available to gather these log files for analysis.

Related information:

 [Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5](#)

Sending information to IBM Support

To reduce the time that it takes to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR) using The Service Request tool.
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data automatically or manually:
 - Collect the data automatically using IBM Support Assistant Lite (ISA Lite). See the links near the beginning of the topic.
 - Collect the data manually. For information about IBM Intelligent Operations Center log files, see the links near the beginning of the topic.
3. Compress the files by using the ZIP or TAR format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
 - The Service Request tool
 - Standard data upload methods: FTP, HTTP
 - Secure data upload methods: FTPS, SFTP, HTTPS
 - Email

All of these data exchange methods are explained on the IBM Support site.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
 - a. Change to the /fromibm directory.
`cd fromibm`
 - b. Change to the directory that your IBM technical-support representative provided.
`cd nameofdirectory`
3. Enable binary mode for your session.
`binary`
4. Use the **get** command to download the file that your IBM technical-support representative specified.
`get filename.extension`
5. End your FTP session.
`quit`

Known problems and solutions

This section contains a list of commonly occurring problems and a solution for each item.

Key performance indicator processing stops after a period

In the IBM Intelligent Operations Center, key performance indicator (KPI) processing occasionally stops after a period, for example, overnight. For information about resolving the problem, see the link at the end of the topic to the *Key performance indicator processing stops after a period of time* troubleshooting technote.

Portlets not populated with data when security settings change

If portlets are not populated with KPI, activity or resource data as you expect, check your port settings. If you use the system properties table to change HTTPS settings and you do not change port settings accordingly, there will be a problem populating portlets with data.

Cognos report connection error

If you receive a Cognos report connection error, refresh the page.

Cognos reports are not displaying correctly

If the Cognos reports do not display correctly when you open the Supervisor: Reports or Operator: Reports page, refresh the page.

If, after you refresh the page, Cognos reports are still not displaying correctly, the Cognos application server clusters might be stopped. Log on to the WebSphere Application Server administrative console and check the status of the WebSphere Application Server clusters. If the status of a cluster shows a red X, select that cluster and press **Start**.

No data found for Cognos reports

If the Cognos reports do not display correctly and you receive a No data found message, data for your selection criteria might not exist in the database. Redefine your selection criteria. For example, clear the **From Date** and **To Date** fields on the custom report, and click **Update**. Then copy the report URL and paste it into the Cognos portlet.

Report is not displayed when you copy the report URL using the Report URL button

As a sample user, if you copy the report URL using the **Report URL** button and then go directly to the Reports portlet page, the report does not display. To fix this issue, press **F5** to refresh, and the report displays correctly.

Edited resource is not displayed in the Details portlet

If you edit a resource in Tivoli Service Request Manager while Tivoli Netcool/Impact is not available, the resource might not be displayed in the Details portlet. For example, if you right-click an event on the **Events and Incidents** tab, and then click **View Nearby Resources**, the edited resource might not be displayed. To resolve the issue, edit the resource again in Tivoli Service Request Manager.

Status of logged out users not displayed correctly in the Contacts portlet

The status of users who are logged on is displayed in the Contacts portlet. If a user who is logged on closes the browser window or logs off from WebSphere Portal, the status of that user is still displayed as logged on until the session expires. However, any messages that are sent to that user, after the user closed the browser window, or logged off, are not delivered. Consequently, an error message is displayed to the user who is trying to send the message. To ensure that your status is updated immediately in the Contacts portlet, log off by clicking **File > Log Out**.

Selecting Update more than once on the Supervisor reports page

On the Supervisor: Reports page in the IBM Intelligent Operations Center user interface, when you select **Update** without making any changes, the **From Date** and **To Date** fields are populated with today's date. If you select **Update** again without making any changes, the message No data found is displayed.

This behavior happens because the **From Date** and **To Date** fields are populated automatically.

Lengthy headlines cause reports charts to be unusable

Event headlines that exceed 20 to 30 characters can affect how the **All Events, by Headline** pie chart report is displayed, making the chart unusable. Because the event headlines label the pie chart sections and the pie chart shrinks to accommodate the labels, the pie chart image becomes too small to distinguish among the various sections.

Unexpected results in the browser time zone conversion


Unexpected results in the browser time zone conversion could be caused by incorrect time zone coding in the Common Alerting Protocol (CAP) event. For more details, see the link at the end of the topic.

Related concepts:

“Using CAP for KPI events” on page 92

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

Related information:

 Key performance indicator processing stops after a period of time troubleshooting technote

Connection errors when installing IBM Intelligent Operations Center

What to do when a SOAPException message is issued when IBM Intelligent Operations Center is being installed.

The connection to a server has been lost when a message similar to the following is issued:

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

If this happens, stop and restart the servers. Then restart the installer or retry the installation command.

IPv6 networking does not start

If IPv6 networking does not start on a server, the `/etc/modprobe.conf` file might require changes.

About this task

This problem can occur when upgrading VMWare to release 5.

Procedure

1. Edit the `/etc/modprobe.conf` file.
2. Change the following line:
`alias ipv6 off`

to

```
# alias ipv6 off
```

3. Change the following line:
`options ipv6 disable=1`

to

```
# options ipv6 disable=1
```

4. Save the file.
5. Restart the server.

Tivoli Service Request Manager does not start

What to do if Tivoli Service Request Manager cannot be started by the Platform Control Tool and is shown by the System Verification Check tool as working.

About this task

To restart Tivoli Service Request Manager, do the following.

Procedure

1. Stop all services using the Platform Control Tool.
2. Shut down and restart the event server.
3. Start all services using the Platform Control Tool.

Cannot create a new page for the user interface

Resolve a problem which occurs when creating a new page if you are working with Microsoft Internet Explorer 9.

About this task

This problem can occur when trying to create a new page from the **Administration** page or from any of the **Citywide** user pages. The new page does not load. To eliminate the problem, switch the browser to **Compatibility View** temporarily. You must ensure that you switch off **Compatibility View** after you have created the new page as the IBM Intelligent Operations Center does not support Internet Explorer 8 or Internet Explorer 9 Compatibility View.

Procedure

1. Open Internet Explorer 9.
2. Log on to IBM Intelligent Operations Center as administrator.
3. Click **Administration > Portal User Interface > Manage Pages**.
4. On the top toolbar of the browser, click **Tools**.
5. From the menu, select **Compatibility View**.
6. Enter citywide in the search box.
7. When the search returns, click on **citywide**.
8. Click **New Page**.
9. When the new page loads, return to the browser toolbar and deselect **Compatibility View**.

Related concepts:

“Supported browsers” on page 13

The IBM Intelligent Operations Center solutions interface supports a number of browsers. Some browsers can be used with limitations.

Accessibility workarounds for portlets

There are workarounds for accessibility issues that relate to some of the IBM Intelligent Operations Center portlets:

- In the Details portlet and the Notifications portlet, to access the pop-up menu, use the following keyboard controls:

Windows

Press the dedicated menu key.

Mac Choose the appropriate option depending on whether you have a numeric keypad:

- If you have a numeric keypad, ensure that Mouse Keys is enabled, and then press Ctrl+5.
 - If you do not have a numeric keypad, enable Mouse Keys, and then press Ctrl+I.
- To open the Add Event window, in the Details portlet, click the **Events and Incidents** tab, or press the Tab key; the screen reader reads the names of the tabs. Then choose the appropriate keyboard controls from the list.

Mozilla Firefox

Ctrl+Alt+V

Safari fn+control+option+V

Internet Explorer

Ctrl+Alt+V

- In the Details portlet, in the Add Event window, the screen reader does not read the following values:
 - **Effective date**
 - **Effective time**

- Onset date
- Onset time
- Expiration date
- Expiration time

Accessibility workaround for selecting dates in the Reports portlet

In the Reports portlet, you cannot select dates from the calendar using the keyboard.

About this task

In the Reports portlet, to configure a predefined report, you must enter a date or a range of dates. However, the calendar date picker is not accessible by keyboard. The calendar is displayed, but you cannot select a date from the calendar using the keyboard. Selecting dates from the calendar only works if you use a mouse.

To work around this issue, complete the following steps to enter the dates manually using the keyboard.

Procedure

1. In the Reports portlet, select the predefined report along the bottom of the page and click **Configure the report**.
2. In the **From date** field, enter the date for which you are viewing information. If you are entering a date range, this date is the beginning date.
3. In the **To date** field, enter the last date in the range of dates for the report information.
4. Click **View the report**.

New events are not displayed in the Details portlet

If new events are not displayed in the Details portlet, a number of steps are available to resolve the issue.

About this task

If the first step does not resolve the issue, proceed to the next step. Continue with each step until the issue is resolved.

Procedure

1. Check the status of the IBM Intelligent Operations Center XML probe
 - a. Log on to the event server as root and enter the command:


```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```
 - b. Check that Connection status OK is displayed at the bottom of the file.
 - c. If a Probe shutting down message is displayed or if the date/time does not match the current server time, complete the following steps:
 - 1) Rename the current log by entering the following command:


```
- mv /opt/IBM/netcool/omnibus/log/ioc_xml.log  
/opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```
 - 2) Restart the probe by entering the following command:


```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile  
/opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```
 - 3) Wait approximately 1 minute, then enter the command:


```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Look for Connection Status OK. If the connection status is not OK, check the file for errors. Connection problems can mean that the object server is down. See step 2 on page 315.

2. If the IBM Intelligent Operations Center XML probe continues shutting down, complete the following steps to check the status of the Tivoli Netcool/OMNIbus database. If the IBM Intelligent Operations Center XML probe does not continue shutting down, proceed to Step 3.

a. Log on to the event server as `ibmadmin` and enter the command:

```
- /opt/IBM/netcool/omnibus/bin/nco_config &
```

b. If prompted to import from `omni.dat`, select **Yes** and click **Finish**.

c. Minimize the process agent window and right-click **NCOMS**.

If the **Connect As** option is available, click it, connect as `root`, and use your topology password.

If you do not see the **Connect As** option, close `nco_config` and, as `ibmadmin`, type the following command to start the NCOMS object server:

```
- /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

If the NCOMS object server does not start, open `/opt/IBM/netcool/omnibus/var`, locate and remove the `NCOMS.pid` file, and type the following command:

```
/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

Note: After you start the NCOMS object server, you must restart the IBM Intelligent Operations Center XML probe. See Step 1 on page 314.

3. Check the status of Tivoli Netcool/Impact.

a. Log on to the event server at `http://EventsHost:9080/nci/login_main.jsp` as `admin`.

If you cannot log on, run the following commands on the event server:

```
su - netcool  
/opt/IBM/netcool/bin/ewas.sh start
```

b. In the **Service Status** window, scroll down and check that the following services are running:

- **EventProcessor**
- **IOC_CAP_Event_Reader**
- **IOC_Notification_Reader**

Note: A green check is displayed beside services that are running.

c. In the **Service Status** window, click the **View Log** icon beside **PolicyLogger**, and check for errors in the log file.

If you find errors in the log, you can view details of the log file at `/opt/IBM/netcool/impact/log/`. For more details, click **PolicyLogger**, set **Highest log level** to **3**, and select the relevant check boxes.

4. Check to see whether events are stuck in one of the WebSphere MQ queues.

a. Use a VNC client to log on to the event server, and enter the following commands to open WebSphere MQ Explorer:

```
xhost +  
su - mqm  
strmqcfcfg &
```

Note: If the Welcome page opens, close it.

b. Expand **IBM WebSphere MQ > Queue Managers > IOC.MC.QM > QueuesLocate**, and select the **Queues** folder.

c. In the **Queues** table, check the **Current Queue Depth** of all queues that begin with **IOC_**. For example, `IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY`.

A queue depth that is greater than 0 for any length of time can indicate an issue.

5. Check that the CAP events reach the IBM Intelligent Operations Center database.

a. Use a VNC client to log on to the data server, and enter the following commands to open the DB2 Control Center:

```
xhost +
su - db2inst1
Db2cc &
```

- b. Click **IOCDB > tables**, right-click **Event** in the **IOC_COMMON** schema, and click **Open**. You see a list of events that are submitted to the system.
- c. Check to ensure that events are in the database.

Note: You might need to fetch more rows, depending on how many events are in the system.

6. To set tracing on the portal server, follow these steps:
 - a. Log on to the administrative console at `http://app-host:9060/ibm/console`, where `app-host` is the fully qualified host name of the application server.
 - b. Click **Troubleshooting > Logs and Trace**.
 - c. Click **WebSphere_Portal > Change log level details**.
 - d. Click the **Runtime** tab, paste in the following command, and click **OK**.
- e. To view a log, enter the following command:

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all

cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

For more information about viewing logs, see the related concept link at the end of the topic.

Related concepts:

“Enabling traces and viewing log files” on page 279

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics give some guidance on how to access log files.

Third-party server not responding

If you receive the Third-party server not responding error message after you log on to the WebSphere Portal portal, check the status of the WebSphere Portal.

Procedure

1. Log on to the management server as `ibmadmin` and type the following command:

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status wpe topology_password
```

If the portal is running, a message similar to the following is displayed:

```
Executing query command.....completed.
IBM WebSphere Portal Extend [ on ]
Command completed successfully.
```

2. If the portal is not running, type `./iopmgmt.sh start wpe topology_password`.

Authentication mechanism not available

If you receive the HPDIA0119W Authentication mechanism is not available error message after you log on to the WebSphere Portal, check the status of the Tivoli Directory Server and the Tivoli Directory Server Proxy for the application server.

Procedure

1. Log on to the management server as `ibmadmin` and type the following commands:

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status tds topology_password
```

If the server is running, a message similar to the following example is displayed:


```
Executing query command.....completed.
IBM Tivoli Directory Server [ on ]
Command completed successfully.
```

2. If the server is not running, type `./iopmgmt.sh start tds topology_password`
3. If the server is not running after you complete Steps 1 on page 316 and 2, log on to the management server as `ibmadmin` and type the following commands:

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status tdspxyapp topology_password
```

If the server is running, a message similar to the following example is displayed:

```
Executing query command.....completed.
IBM Tivoli Directory Server [ on ]
Command completed successfully.
```

4. If the server is not running, type `./iopmgmt.sh start tdspxyapp topology_password`

No activities are displayed in the My Activities portlet

If you cannot see any activities in the My Activities portlet, there are several possible causes, which are described in the following sections.

Troubleshooting with the sample data

Use the sample data to create an event and use the results to narrow down the possible cause of activities not being displayed.

Procedure

1. Log on to the IBM Intelligent Operations Center administrative interface as `wpsadmin`.
2. Create a “Hurricane Approaching” event:
 - a. In the Map portlet, right-click the map, and then click **Add Event**.
 - b. For **Event type**, select **Hurricane Approaching**. The other fields are automatically pre-populated.
 - c. For **Urgency**, select **Expected**.
 - d. Keep the default values for the other event parameters, and click **OK**.

The parameters for the “Hurricane Approaching” event are mapped to a sample standard operating procedure in the standard operating procedure selection matrix.

3. After approximately 5 minutes, verify that a new activity that corresponds to the “Hurricane Approaching” event is displayed in the My Activities portlet.

Results

- If an activity that corresponds to the “Hurricane Approaching” event is not displayed in the My Activities portlet, the problem of activities not being displayed for another user might be because of a problem with Tivoli Service Request Manager.
- If an activity that corresponds to the “Hurricane Approaching” event is displayed in the My Activities portlet, the problem of activities not being displayed for another user might be because of one of the following reasons:
 - The user permissions are not configured correctly.
 - A standard operating procedure is not configured correctly.
 - The standard operating procedure selection matrix is not configured correctly.

Related reference:

“Sample standard operating procedures, workflows, and resources” on page 133
Sample standard operating procedures, workflows, and resources are provided when you install IBM Intelligent Operations Center Version 1.5.

Verifying the status of Tivoli Service Request Manager

If no activity is displayed in the My Activities portlet when you create an event using the sample data, use the following procedure to troubleshoot Tivoli Service Request Manager.

Before you begin

Ensure that the Tivoli Service Request Manager administrative password has been encrypted correctly. For more information, see the link at the end of the procedure.

About this task

Choose one of the following options.

Procedure

- Use the Platform Control Tool to check the status of Tivoli Service Request Manager:
 1. Log on to the event server as `ibmadmin` with the `putty` command.
 2. Go to the `opt/IBM/ISP/mgmt/scripts` directory.
 3. Use the Platform Control Tool to get the status of Tivoli Service Request Manager, and to stop and start Tivoli Service Request Manager. For more information about running the Platform Control Tool, see the links at the end of the procedure.
- Alternatively, to manually restart Tivoli Service Request Manager, do the following steps:

1. Log on to the event server as `ibmadmin` with the `putty` command.
2. To stop Tivoli Service Request Manager, enter the following commands:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
./stopServer.sh MXServer1 -user waswebadmin -password password
./stopNode.sh -user waswebadmin -password password
../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password password
```

where *password* is the topology password.

3. To start Tivoli Service Request Manager, enter the following commands:

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
../../ctgDmgr01/bin/startManager.sh
./startNode.sh -user waswebadmin
./startServer.sh MXServer1
exit
```

Related tasks:

“Querying the status of the services” on page 191

The Platform Control Tool is available to determine the status of IBM Intelligent Operations Center services.

“Starting the services” on page 185

The Platform Control Tool is available to start the services running on IBM Intelligent Operations Center servers.

“Stopping the services” on page 188

The Platform Control Tool is available to stop the IBM Intelligent Operations Center services.

“Encrypting the Tivoli Service Request Manager administrative password” on page 56

Use the following procedure to encrypt the Tivoli Service Request Manager administrative password in Tivoli Netcool/Impact.

Verifying user permissions

Verify that a user has permission to view activities that are associated with a standard operating procedure.

Procedure

1. To open the Standard Operating Procedures portlet, in the WebSphere Portal Administration interface, click **Intelligent Operations > Customization Tools > Standard Operating Procedures**.
2. To open the Standard Operating Procedure Selection Matrix application, click **Standard Operating Procedures Selection Matrix**.
3. In the **SoP Name** column, locate the name of a standard operating procedure that you want to verify user permissions for.
4. Next to the **SoP Name** field, click the **Detail Menu** icon, and then click **Go To Standard Operating Procedure**.
5. Next to the **Owner Group** field, click the **Detail Menu** icon, and then click **Go To Person Groups**.
6. Verify that the user is a member of the person group.

What to do next

If a user is not a member of the person group, take one of the following actions:

- Do not give the user permission to view activities that are associated with the standard operating procedure.
- Add the user to the person group so that the user can see all activities that are assigned to the person group.
- Add the user to another person group that is associated with the standard operating procedure.

For more information about configuring users, see the link at the end of the task.

Related tasks:

“Configuring new users in Tivoli Service Request Manager” on page 121

When you add a user in IBM Intelligent Operations Center, assign permissions and person groups for the user in Tivoli Service Request Manager.

Verifying the association of a workflow with a standard operating procedure

Create an event whose parameters match a set of selection criteria that you define in the standard operating procedure selection matrix. Verify that the associated workflow activities are displayed in the My Activities portlet.

About this task

For more information about each of the following steps, see the links at the end of the procedure.

Procedure

1. Create a workflow.
2. Create a standard operating procedure, and associate it with the workflow that you created in the previous step.
3. Create an entry for the standard operating procedure in the standard operating procedure selection matrix.
4. In the Map portlet, create an event that matches the parameters that you defined in the standard operating procedure selection matrix.
5. Verify that the associated workflow activities are displayed in the My Activities portlet.

What to do next

If no activities are displayed in the My Activities portlet, check that you have configured the workflow, the standard operating procedure, the standard operating procedure selection matrix, and the event correctly. If the configuration is correct, check the Tivoli Netcool/OMNIBus policy log file, and the Tivoli Service Request Manager log files.

Related concepts:

[“Map” on page 264](#)

Use the Map portlet to see events and resources on a map.

[“My Activities” on page 269](#)

The My Activities portlet displays a dynamic list of activities that are owned by the group of which the user, who is logged on to the interface, is a member.

Related tasks:

[“Creating workflows” on page 124](#)

In Tivoli Service Request Manager, you can create workflows that you can include as automated tasks in your standard operating procedure activities.

[“Creating standard operating procedures” on page 124](#)

Create a standard operating procedure, and assign it to an owner group. Users are assigned to an owner group through their membership of a person group.

[“Defining parameters in the standard operating procedure selection matrix” on page 126](#)

In the standard operating procedure selection matrix, define the event parameters that determine whether a standard operating procedure is selected for a particular event.

Checking the log files

Check the Tivoli Netcool/OMNIBus policy log file, and the Tivoli Service Request Manager log file.

Procedure

- Check the Tivoli Netcool/OMNIBus policy log file:
 1. Enable the Tivoli Netcool/OMNIBus policy log file. For information about enabling and using the log file, see the link at the end of the procedure.
 2. In the Tivoli Netcool/OMNIBus policy log file, to locate an event, search for `CallMaximoEnterpriseServices`. The Tivoli Netcool/OMNIBus policy log file parses events by parameter, for example, `Category`, and `Severity`, and lists each event with its associated work order ID. You can match events against the standard operating procedure selection matrix. If an event is not listed in the Tivoli Netcool/OMNIBus policy log file, the probable reason is that no standard operating procedure matches the event parameters.

3. Search for server error 500, which indicates a Tivoli Service Request Manager server error. If you see this error, check the Tivoli Service Request Manager log file. See the link at the end of the procedure.
- Check the Tivoli Service Request Manager log file. For information about enabling and using the log file, see the link at the end of the procedure.

Related tasks:

“Enabling and viewing Tivoli Netcool/Impact log files” on page 282

“Enabling tracing and viewing log files for Tivoli Service Request Manager” on page 280

KPI data is not displayed in the Status or Key Performance Indicator Drill Down portlets

If KPI data is not displayed in the Status or Key Performance Indicator Drill Down portlets, follow the steps in the procedure to resolve the problem.

Procedure

1. To check the status of IBM WebSphere Business Monitor, log on to the WebSphere Application Server administration console. For more information about accessing administration consoles, go to the link at the end of the topic.
2. If IBM WebSphere Business Monitor is stopped, restart it. If IBM WebSphere Business Monitor is not stopped, first stop it, and then restart it. If the issue is not resolved, then do step 3.
3. Check IBM WebSphere Business Monitor logs to investigate and resolve any issues with IBM WebSphere Business Monitor. For more information about checking the logs, go to the link at the end of the topic.
4. When all IBM WebSphere Business Monitor issues are resolved, log on to the WebSphere Application Server administration console to restart IBM WebSphere Business Monitor.

Related concepts:

“Application server log files” on page 279

Use the following procedures to enable traces and view logs for some of the systems on the application server.

“Administration Consoles” on page 192

Use the Administration Consoles portlet to administer the services provided by the solution.

Events are not updated in the Status or Key Performance Indicator Drill Down portlets

If KPI event data is not updated in the Status or Key Performance Indicator Drill Down portlets, follow the steps in the procedure until you resolve the issue.

Procedure

1. To confirm that KPI event updates are reaching the IBM Intelligent Operations Center, go to the *New events are not displayed in the Details portlet* link at the end of the topic and follow the steps.
2. Confirm that events are reaching IBM WebSphere Business Monitor.
 - a. Log on to the WebSphere Application Server administration console. For more information about accessing administration consoles, go to the link at the end of the topic.
 - b. Click **Troubleshooting > Monitor Models > Failed Event Sequences**. Delete any KPI events that are displayed on this page.
 - c. Restart IBM WebSphere Business Monitor.
 - d. Click **Applications > Monitor Services > Recorded Events Management > Enable/Disable Events Record** and enable event recording.

- e. Click **Applications > Monitor Services > Recorded Events Management > Events Management**.
Check on this page that there are at least two events created for every KPI event that is sent to the IBM Intelligent Operations Center.
3. Confirm that KPI event updates are reaching the Key Performance Indicators portlet. For more information about the Key Performance Indicators portlet, go to the link at the end of the topic. If you see KPI values updated in the Key Performance Indicators portlet, then the values are updated in IBM WebSphere Business Monitor.

Related concepts:

“Administration Consoles” on page 192

Use the Administration Consoles portlet to administer the services provided by the solution.

“Key Performance Indicators” on page 160

Use the Key Performance Indicators portlet to customize Key Performance Indicators (KPIs) and their hierarchical display in the IBM Intelligent Operations Center.

Related tasks:

“New events are not displayed in the Details portlet” on page 314

If new events are not displayed in the Details portlet, a number of steps are available to resolve the issue.

Chapter 10. Reference

These topics contain additional reference information to help you.

Products and components included with IBM Intelligent Operations Center

The IBM Intelligent Operations Center solution installs a number of software products and components.

The software products and components and the servers they are installed on are shown in Table 100.

Table 100. Products installed with IBM Intelligent Operations Center

| Product | Application server | Data server | Event server | Management server |
|---|--------------------|---------------|---------------|-------------------|
| IBM WebSphere Business Monitor 7.5 | installed | not installed | not installed | not installed |
| IBM Cognos Business Intelligence 10.1.1 | installed | not installed | not installed | not installed |
| DB2 Enterprise Server Edition with DB2 Spatial Extender 9.7.0.5 | not installed | installed | not installed | installed |
| Semantic model services | not installed | not installed | not installed | installed |
| IBM ILOG [®] CPLEX [®] Optimization Studio 12.4 | installed | not installed | not installed | not installed |
| Jazz Foundation Server (for Semantic model services) 3.0.1 | not installed | not installed | not installed | installed |
| Lotus Domino 8.5.3.1 | not installed | not installed | installed | not installed |
| Lotus Sametime Standard 8.5.2 + IFR1 | not installed | not installed | installed | not installed |
| Tivoli Access Manager for e-Business 6.1.1.4 | not installed | not installed | not installed | installed |
| Tivoli Composite Application Manager 7.1 | not installed | not installed | not installed | installed |
| Tivoli Directory Integrator 7.1.0.5 | not installed | not installed | not installed | installed |
| Tivoli Directory Server 6.3.0.8 | not installed | installed | not installed | not installed |
| Tivoli Identity Manager 5.1 | not installed | not installed | not installed | installed |
| Tivoli Monitoring 6.2.2.1 | not installed | not installed | not installed | installed |
| Tivoli Netcool/Impact 5.1.1.1 + IF003 | not installed | not installed | installed | not installed |

Table 100. Products installed with IBM Intelligent Operations Center (continued)

| Product | Application server | Data server | Event server | Management server |
|--|--------------------|---------------|---------------|-------------------|
| Tivoli Netcool/OMNIBus 7.3.1.2 and XML probe | not installed | not installed | installed | not installed |
| Tivoli Service Request Manager 7.2.1.2 | not installed | not installed | installed | not installed |
| WebSphere Application Server 1.1.0.0 Feature Pack for Web 2.0 and Mobile | installed | not installed | not installed | not installed |
| WebSphere Application Server Network Deployment 7.0.0.21 | installed | not installed | not installed | installed |
| WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager | not installed | not installed | installed | not installed |
| WebSphere Message Broker 8.0 | not installed | not installed | installed | not installed |
| WebSphere MQ 7.0.1.7 | not installed | not installed | installed | not installed |
| WebSphere Operational Decision Management 7.5.1 (Rules Engine) | installed | not installed | not installed | not installed |
| WebSphere Portal Enable 7.0.0.2 | installed | not installed | not installed | not installed |

Processes running under the root account

After cyber hygiene is run, some processes still must run under the root account.

Processes running under the root account can be vulnerable if a user or process can obtain root privileges through privilege escalation. Normally this is only a problem for services processing requests originated by a user. User-originated requests can contain maliciously configured input that can compromise the server. Services processing user requests are systems providing user interfaces or accessible application programming interfaces (APIs).

Linux daemons are not normally at risk since they usually only start, stop, or respond to well-defined system events. In many cases these daemons must run as the root account so they can control other processes or respond to critical system events. As long as a user-accessible server itself is not running as root, daemons running under the root account do not present as serious an exposure.

With the exception of Tivoli Netcool/OMNIBus, all product servers in IBM Intelligent Operations Center are configured under IDs that do not have system privileges. Tivoli Netcool/OMNIBus provides monitoring and management services across all IBM Intelligent Operations Center hosts and servers.

Table 101 lists the processes that continue running as the root account after cyber hygiene is run.

Table 101. IBM Intelligent Operations Center environment processes running as root

| Server | Product | Process Name | Explanation |
|---|---|--|--|
| data server and management server | DB2 | db2wdog | This daemon process receives system events and propagate them to multiple child processes. The db2wdog process manages the db2sync processes and requires root level management. |
| data server and management server | DB2 | db2chkpwd | This daemon authenticates the user ID and password of the user or application connecting to a database. The db2chkpwd process needs to read the /etc/shadow password file. |
| data server and management server | DB2 | /opt/IBM/DB2/bin/db2fmc | This daemon serves as a fault monitoring coordinator. It must run as root to monitor all DB2 instances. |
| data server and management server | DB2 | /usr/sbin/rcst/bin/rmcd and /usr/sbin/rcst/bin/IBM.ConfigRMd | These commands manage the high availability solution for DB2. They need access to all databases on the servers configured for high availability. |
| event server | IBM Tivoli Monitoring agents for Lotus Domino | kgbagent, kgbclient, kslagent | These monitoring agents need to run as root to track Lotus Domino server activity. |
| application server, event server, and management server | IBM HTTP Server | httpd -d, http -f | Linux requires root access to listen on ports less than 1024. Standard HTTP ports are 80 through 443. IBM Intelligent Operations Center uses port 82. The httpd -d and http -f processes must run as root. Any alternate configuration is the responsibility of the installation as part of comprehensive network and security policy and configuration. |
| data server | IBM Tivoli Monitoring agents | klzagent, kcawd | These are monitoring and management agent processes. These processes monitor operating system and application processes and resources. |
| application server | IBM Tivoli Monitoring agents | klzagent, kcawd, khtagent, kynagent | These are monitoring and management agent processes. These processes monitor operating system and application processes and resources. |
| event server | IBM Tivoli Monitoring agents | klzagent, kcawd, khtagent, kynagent, kmcrca, kgbagent, kgbstart.sh, kgbclient, kslagent, kmqagent, /opt/IBM/ITM/JRE/1x8266/bin/java | These are monitoring and management agent processes. These processes monitor operating system and application processes and resources. |
| management server | IBM Tivoli Monitoring agents | cms, kdsmain, KfwServices, klzagent, kcawd, kynagent, /opt/IBM/ITM/1i6263/iw/java/jre/bin/java, /opt/IBM/ITM/1i6263/iw/java/bin/java | These are monitoring and management agent processes. These processes monitor operating system and application processes and resources. |
| event server | Tivoli Netcool/OMNIBus | /usr/ibm/common/acsi/jre/bin/java, /opt/IBM/netcool/omnibus/platform/linux2x26/bin/nco_pad | The nco_pad process is the process agent daemon that monitors all the process agents. The daemon requires access to system resources. The process agent daemon does not present a user interface. It only manages other processes. |

Cyber hygiene exceptions

Once cyber hygiene is run, there remain known exceptions to the preferred security configuration.

An ideal configuration would not have exceptions to best practice settings. However, most systems have exceptions. These exceptions do not present a significant risk, but might be problematic if not understood. For example, some programs might have to run with the **suid** bit set.

Security administrators need to understand the exceptions so they can verify if their system has been compromised. When scanning the system administrators can understand intended exceptions as opposed to malware.

Table 102. Cyber hygiene exceptions to the preferred security configuration

| Vulnerability | Server | Instance | Explanation |
|--|-------------|----------|---|
| GEN000360: GID set to value in the system range for Linux (0-499). | data server | dasadm1 | The dasadm1 Group ID (GID) is set to 102. This is the administration group for the DB2 runtime instance IDs. This group is automatically created when DB2 is installed. |

File permissions requiring system administrator evaluation

Cyber hygiene does not make changes for exposures in all file permissions and ownership. Some of these must be evaluated and remediated by system administrators since automated changes could make some system functions inoperable.

The cyber hygiene scripts log information on potentially affected resources. System administrators can review these findings and make appropriate system changes.

Findings files are located in the `/var/BA15/CH/results` directory on each IBM Intelligent Operations Center server. The file name is `scanrem-combined-log-date-time.log`. The timestamp indicates when cyber hygiene was run.

Table 103 lists vulnerabilities and recommended actions requiring review.

Table 103. Vulnerabilities requiring evaluation by the system administrator

| STIGID | Description | Severity | Recommendation |
|-----------|--|----------|---|
| GEN001220 | Files, applications, and directories in system directories must be owned by a system account or an application account. | II | Review the ownership of the resource and manually change or document as required. |
| GEN001240 | Files, applications, and directories in system directories must be owned by a system group or an application group. | II | Review the group ownership of the resource and manually change or document as required. |
| GEN001500 | The home directory, listed for a user in the <code>/etc/passwd</code> file, should be owned by a user. | II | Review the ownership of the home directory and manually change the ownership, or document why it cannot be changed. |
| GEN001520 | The home directory, listed for a user in the <code>/etc/passwd</code> file, should be owned by the user's primary group. | II | Review the group ownership of the home directory and manually change the group ownership, or document why it cannot be changed. |
| GEN001560 | Files in the home directory, other than start up files, should have permissions no greater than 750. | III | Change permissions if exceptions are not already documented. |
| GEN002520 | Public directories must be owned by the root account or an application user ID. | II | Review ownership and assign as appropriate. |
| GEN002540 | Public directories must be owned by the root, sys, bin, or an application group. | II | Review group ownership and assign as appropriate. |

Product and component security certifications

Some of the products and components included as part of the IBM Intelligent Operations Center solution have security certifications.

Table 104. Security certifications of products installed with IBM Intelligent Operations Center

| Product | Common criteria | | FIPS 140-2 | | IPV6 |
|---|-----------------|---------------------|------------|------------|------|
| | Release | Level | Release | Certified? | |
| IBM WebSphere Business Monitor | None | None | 7.5 | Yes | Yes |
| IBM Cognos Business Intelligence | 10.1.1 | None | None | None | Yes |
| DB2 Enterprise Server Edition with DB2 Spatial Extender | 9.7 | EAL4+ALC_FLR.1 | 9.1 FP2 | Yes | Yes |
| IBM HTTP Server | 7.0.0.19 | | 7.0 | Yes | Yes |
| Lotus Domino | None | None | 8.0.1 | Yes | Yes |
| Lotus Sametime Standard | None | None | 8.5 | Yes | Yes |
| Tivoli Access Manager for e-Business | 6.0 FP3 | EAL3+ALC_FLR.1 | 6.0 | Yes | Yes |
| Tivoli Composite Application Manager | None | None | None | None | Yes |
| Tivoli Directory Integrator | None | None | 7.0 | Yes | Yes |
| Tivoli Directory Server | 6.2 | EAL4+ALC_FLR.1 | 6.1 | Yes | Yes |
| Tivoli Identity Manager | 5.0 | EAL3+ALC_FLR.1 | None | None | Yes |
| Tivoli Monitoring | None | None | 6.2.0.1 | Yes | Yes |
| Tivoli Netcool/Impact | None | None | 5.1 | Yes | Yes |
| Tivoli Netcool/OMNIBus and XML probe | 7.1 | EAL2 | All | Yes | Yes |
| Tivoli Service Request Manager | None | None | All | Yes | Yes |
| WebSphere Application Server Network Deployment | 6.1.0.2 | EAL4+ALC_FLR.1 | All | Yes | Yes |
| WebSphere Application Server for Tivoli Service Request Manager | 6.1.0.2 | EAL4+ALC_FLR.1 | All | Yes | Yes |
| WebSphere Message Broker | 6.0.0.3 | EAL4+ALC_FLR.2 (de) | 6.1 | Yes | Yes |
| WebSphere MQ | 6.0.1.1. | EAL4+ALC_FLR.2 | All | Yes | Yes |
| WebSphere Operational Decision Management (Rules Engine) | None | None | None | None | Yes |
| WebSphere Portal Enable | 5.0 | EAL2 | All | Yes | Yes |

Products with FIP 104-2 certification is normally due to the use of IBM Crypto for C and Java modules. The certificate numbers for these products are shown in Table 105.

Table 105. FIPS 140-2 certificates

| Module | Certificate number |
|---|--------------------|
| IBM Crypto for C (V8.0.0) | 1433 |
| IBM CryptoLite for Java (V4.2) | 910 |
| IBM CryptoLite for C (V4.5) | 899 |
| IBM Java JCE 140-2 Cryptographic Module | 497 |
| IBM Java JSSE FIPS 140-2 Cryptographic Module | 409 |
| IBM SSL Lite for Java | 406 |

Related information:

 Common Criteria: <http://www.commoncriteriaportal.org/>

 Security Evaluations for IBM Products

PDF library

The product documentation is available in PDF for convenient printing.

- IBM Intelligent Operations Center documentation
-

Glossary

This glossary includes terms and definitions for IBM Intelligent Operations Center.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

[“A”](#) [“B”](#) on page 329 [“C”](#) on page 329 [“D”](#) on page 330 [“E”](#) on page 330 [“F”](#) on page 331 [“G”](#) on page 331 [“H”](#) on page 331 [“I”](#) on page 331 [“J”](#) on page 331 [“K”](#) on page 332 [“L”](#) on page 332 [“M”](#) on page 333 [“N”](#) on page 333 [“O”](#) on page 333 [“P”](#) on page 333 [“R”](#) on page 334 [“S”](#) on page 334 [“T”](#) on page 335 [“U”](#) on page 335 [“V”](#) on page 336 [“W”](#) on page 336 [“X”](#) on page 337

A

Abstract Syntax Notation One (ASN.1)

The international standard for defining the syntax of information data. It defines a number of simple data types and specifies a notation for referencing these types and for specifying values of these types. The ASN.1 notations can be applied whenever it is necessary to define the abstract syntax of information without constraining in any way how the information is encoded for transmission.

access control list (ACL)

In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

ACL See access control list.

administrator permission

The authority granted to an administrator to give them access to create, configure, and delete portal resources or users. This authority is granted by membership of a user role group.

aggregation KPI

A KPI value that is calculated from a metric using an aggregation function.

alert A message that signals an event or key performance indicator (KPI) status change.

alert trigger

A predefined key performance indicator (KPI) value change that causes an alert notification to be sent to the Coordinator - Alerts portlet.

APAR See authorized program analysis report.

ASN.1 See Abstract Syntax Notation One.

asynchronous

Pertaining to events that are not synchronized in time or do not occur in regular or predictable time intervals.

attribute

A characteristic or trait of an entity that describes the entity; for example, the telephone number of an employee is one of the employee attributes.

authenticated portal user

A user that is a member of an umbrella group within WebSphere Portal authenticated with a profile containing a password and user ID.

authentication

A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures.

authorization

The process of granting a user, system, or process either complete or restricted access to an object, resource, or function.

authorization permission

Access to a portal, resource, or data associated with membership of a group.

authorized program analysis report (APAR)

A request for correction of a defect in a supported release of a program supplied by IBM.

B**base map**

A map that depicts background reference information such as landforms, roads, landmarks, and political boundaries, onto which other thematic information is placed. A base map is used for locational reference and often includes a geodetic control network as part of its structure.

C

cache Memory used to improve access times to instructions, data, or both. Data that resides in cache memory is normally a copy of data that resides elsewhere in slower, less expensive storage, such as on a disk or on another network node.

CAP See Common Alerting Protocol.

cloud application

An application that is extended to be accessible through the Internet. Cloud applications use large data centers and powerful servers that host web applications and web services.

Common Alerting Protocol (CAP)

A simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks.

common widget

A widget provided by IBM that is not associated with a particular product. See also widget.

configuration

1. The manner in which the hardware and software of a system, subsystem, or network are organized and interconnected.
2. The process of describing to a system the devices, optional features, and program products that have been installed so that these features can be used. See also customization.

CSV file

A text file that contains comma-separated values. A CSV file is commonly used to exchange files between database systems and applications that use different formats.

customization

1. The modification of a portal page or portlet by a user. WebSphere Portal enables a user to customize a portal page by modifying the page layout and by selecting which portlets will display per device. See also personalization.
2. The process of describing optional changes to defaults of a software program that is already installed on the system and configured so that it can be used. See also configuration.

D

dashboard

1. A web page that can contain one or more widgets that graphically represent business data.
2. An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data access permission

Access to data in a particular category, for example, medical and public health data, or environmental data. This access is associated with a data category group.

data category group

A group whose members have access to a specific category of data, for example, medical and public health data, or environmental data. Membership of a data category group is assigned to give a user the appropriate level of access to data. Each user is added as a member of the appropriate group or groups.

domain

An individual division of a major operation, which generally matches the organization structure and the expertise of the people involved. For example, a city authority is divided into departments dealing with transportation, water, and public safety.

E

EAR See enterprise archive.

EJB See Enterprise JavaBeans.

enterprise archive (EAR)

A specialized type of JAR file, defined by the Java EE standard, used to deploy Java EE applications to Java EE application servers. An EAR file contains EJB components, a deployment descriptor, and web archive (WAR) files for individual web applications. See also Java archive.

Enterprise JavaBeans (EJB)

A component architecture defined by Sun Microsystems for the development and deployment of object-oriented, distributed, enterprise-level applications (Java EE).

event A significant occurrence that happens at a given place and time. See also incident.

event correlation

The process of analyzing event data to identify patterns, common causes, and root causes. Event correlation analyzes the incoming events for predefined states, using predefined rules, and against predefined relationships.

expression KPI

A KPI that has its value calculated from the values of the other KPIs.

Extensible Markup Language (XML)

A standard metalanguage for defining markup languages that is based on Standard Generalized Markup Language (SGML).

F

filter form

A form that can be used to select content to be displayed on the map and list.

G

GDDM

See Graphical Date Display Manager.

geographical information system (GIS)

A complex of objects, data, and applications that is used to create and analyze spatial information about geographic features.

geospatial

Pertaining to the geographical characteristics of the Earth.

GIS See geographical information system.

Graphical Date Display Manager (GDDM)

An IBM computer-graphics system that defines and displays text and graphics for output on a display or printer.

group A collection of users who can share access authorities for protected resources.

H

heap In Java programming, a block of memory that the Java virtual machine (JVM) uses at run time to store Java objects. Java heap memory is managed by a garbage collector, which automatically de-allocates Java objects that are no longer in use.

hover help

Explanatory text that can be viewed by moving a cursor over a graphical user interface (GUI) item such as an icon, field, or text string. Hover help can contain rich text and links.

I

incident

An event that is not part of the standard operation of a service and causes or can cause a disruption to or a reduction in the quality of services and customer productivity. See also event.

integration

The software development activity in which separate software components are combined into an executable whole.

ISO model

A set of rules for data communication, sanctioned by the International Organization for Standardization (ISO). The ISO protocols enable systems supplied by different vendors to connect and communicate. They are the basis of the open systems interconnection (OSI) standards.

J

J2EE See Java Platform, Enterprise Edition.

JAR See Java archive.

Java archive (JAR)

A compressed file format for storing all of the resources that are required to install and run a Java program in a single file. See also enterprise archive.

Java EE

See Java Platform, Enterprise Edition.

Java Naming and Directory Interface (JNDI)

An extension to the Java platform that provides a standard interface for heterogeneous naming and directory services.

Java Platform, Enterprise Edition (J2EE, Java EE)

An environment for developing and deploying enterprise applications, defined by Oracle. The Java EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multitiered, web-based applications. (Sun)

JavaScript Object Notation (JSON)

A lightweight data-interchange format that is based on the object-literal notation of JavaScript. JSON is programming-language neutral but uses conventions from languages that include C, C++, C#, Java, JavaScript, Perl, Python.

Java virtual machine (JVM)

A software implementation of a processor that runs compiled Java code (applets and applications).

JNDI See Java Naming and Directory Interface.

JSON See JavaScript Object Notation.

JVM See Java virtual machine.

K**keyhole markup language (KML)**

An XML grammar and file format for modeling and storing geographic features such as points, lines, images, and polygons.

key performance indicator (KPI)

A quantifiable measure that is designed to track one of the critical success factors of a business process.

KML See keyhole markup language.

KPI See key performance indicator.

KPI model

The part of the monitor model that contains the KPI contexts, which in turn contain key performance indicators and their associated triggers and events.

KPI policy

A policy that determines if an incoming event is a KPI event update, then sends it for processing to generate a KPI update or an alert depending on parameters.

L**latitude**

The angular distance of a place north or south of the earth's equator, usually expressed in degrees and minutes.

layer An overlay that can be placed on the map to provide additional geospatial information.

LDAP See Lightweight Directory Access Protocol.

LDAP Directory Interchange Format (LDIF)

A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF See LDAP Directory Interchange Format.

level of service (LOS)

A qualitative measure used in the transportation industry by traffic engineers to determine the effectiveness of elements of a transportation infrastructure. This measure describes the operational conditions of traffic as defined in the Highway Capacity Manual.

Lightweight Directory Access Protocol (LDAP)

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

linear reference

A location reference marker along a roadway, generally on a shoulder, indicating its location along a route. An example of a marker is a milepost.

location map

A map or plan containing interactive areas that have been defined in the IBM Intelligent Operations Center. Events can be associated with one or more of these areas. For example, a diagram of seating areas in a major sports stadium can be defined so that events that have occurred can be associated with the appropriate area.

logical zone

A logical grouping of assets or events in a geographical area.

longitude

The angular distance of a place east or west of the meridian at Greenwich, England, usually expressed in degrees and minutes.

LOS See level of service.

M

monitoring context instance

Information in IBM WebSphere Business Monitor that is collected at a specific point in time within a monitoring context.

monitor model

A model that describes the business performance management aspects of a business model, including events, business metrics, and key performance indicators (KPIs) that are required for real-time business monitoring.

N

nested KPI

A KPI that is defined as a child of a parent KPI.

O

ontology

An explicit formal specification of the representation of the objects, concepts, and other entities that can exist in some area of interest and the relationships among them.

operations view

A web page containing portlets that can cooperate to facilitate comprehensive information supply and interaction at operations level for monitoring current events and planning future events.

OWL See web ontology language.

P

page In a portal environment, the interface element that contains one or more portlets.

personalization

The process of enabling information to be targeted to specific users based on business rules and user profile information. See also customization.

plug-in

A separately installable software module that adds function to an existing program, application, or interface.

PMR See problem management record.

polygon

In the GDDM function, a sequence of adjoining straight lines that enclose an area.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

portlet

A reusable component that is part of a web application that provides specific information or services to be presented in the context of a portal.

problem management record (PMR)

The number in the IBM support mechanism that represents a service incident with a customer.

R

RDF See Resource Description Framework.

Really Simple Syndication (RSS)

An XML file format for syndicated web content that is based on the Really Simple Syndication specification (RSS 2.0). The RSS XML file formats are used by Internet users to subscribe to websites that have provided RSS feeds.

Representational State Transfer (REST)

A software architectural style for distributed hypermedia systems like the World Wide Web. The term is also often used to describe any simple interface that uses XML (or YAML, JSON, plain text) over HTTP without an additional messaging layer such as SOAP.

resource bundle

1. A class that contains the text for the store pages. Bundle files are created and accessed according to the Java PropertyResourceBundle API.
2. A structured collection of data that provides a key-value mapping for data (resources) used in localizing a program. The values are commonly strings, but may themselves be structured data.

Resource Description Framework (RDF)

A framework for representing information on the web.

REST See Representational State Transfer.

RSS See Really Simple Syndication.

S**Secure Sockets Layer (SSL)**

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

SGML

See Standard Generalized Markup Language.

shape file

A digital file format for geographic information systems software.

single sign-on (SSO)

An authentication process in which a user can access more than one system or application by entering a single user ID and password.

skin An element of a graphical user interface that can be changed to alter the appearance of the interface without affecting its functionality.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet. See also web service.

solution

A combination of products that addresses a particular customer problem or project.

SPARQL

A query language for RDF that is used to express queries across diverse data sources. The W3 specification defines the syntax and semantic of the SPARQL query language.

SSL See Secure Sockets Layer.

SSO See single sign-on.

Standard Generalized Markup Language (SGML)

A standard metalanguage for defining markup languages that is based on the ISO 8879 standard. SGML focuses on structuring information rather than presenting information; it separates the structure and content from the presentation. It also facilitates the interchange of documents across an electronic medium.

Standard Operating Procedure

A procedure defining a sequence of activities that are triggered in response to an event whose parameters meet certain predefined conditions.

Standard Operating Procedure selection matrix

A matrix containing unique sets of event parameters that determine whether a Standard Operating Procedure is initiated for a particular event.

system properties table

A table that stores system-wide configuration data for the IBM Intelligent Operations Center.

T

TAI See trust association interceptor.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

theme The style element that gives a place a particular look. The portal provides several themes, similar to virtual wallpaper, which can be chosen when creating a place.

Transmission Control Protocol/Internet Protocol (TCP/IP)

An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

trigger

A mechanism that detects an occurrence and can cause additional processing in response.

trust association interceptor (TAI)

The mechanism by which trust is validated in the product environment for every request received by the proxy server. The method of validation is agreed upon by the proxy server and the interceptor.

U**Uniform Resource Identifier (URI)**

1. A unique address that is used to identify content on the web, such as a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the web page address, which is a particular form or subset of URI called a Uniform Resource Locator (URL). A URI typically describes how to access the resource, the computer that contains the resource, and the name of the resource (a file name) on the computer.
2. A compact string of characters for identifying an abstract or physical resource.

Uniform Resource Locator (URL)

The unique address of an information resource that is accessible in a network such as the Internet. The URL includes the abbreviated name of the protocol used to access the information resource and the information used by the protocol to locate the information resource.

URI See Uniform Resource Identifier.

URL See Uniform Resource Locator.

user administrator

A person who adds new users and ensures security by giving users membership of role-based authorization groups with appropriate permissions.

user permission

The authority granted to a user to give them access to view and work with portal resources. This authority is granted by membership of a user role group.

user profile

A description of a user that includes such information as user ID, user name, password, access authority, and other attributes that are obtained when the user logs on.

user role group

A group that assigns membership to give a new user the appropriate level of access to the solution. Each new user is added as a member of the appropriate role group. There are different permission levels associated with each role group.

V

Virtual Network Computing (VNC)

A graphical desktop sharing system that uses the remote frame buffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC See Virtual Network Computing.

W

Web Map Service (WMS)

A standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database. The specification was developed and first published by the Open Geospatial Consortium in 1999.

web ontology language (OWL)

A language that is used to explicitly represent the meaning of terms in vocabularies and the relationships between those terms. OWL is intended to be used when the information contained in documents is to be processed by applications, as opposed to situations where the content is to be presented only to humans.

web service

A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available. See also SOAP, Web Service Definition Language.

Web Service Definition Language (WSDL)

An XML-based specification for describing networked services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. See also web service.

widget

A reusable user interface component such as a button, scroll bar, control area, or text edit area, that can receive input from the keyboard or mouse and can communicate with an application or with another widget. See also common widget.

WMS See Web Map Service.

WO See work order.

workflow

A specific set of actions appropriate to a particular set of circumstances. The solution can be customized to trigger appropriate workflows, for example connecting to emergency response systems.

work order (WO)

A record that contains information about work that must be performed.

WSDL

See Web Service Definition Language.

X

XML See Extensible Markup Language.

XML schema

A mechanism for describing and constraining the content of XML files by indicating which elements are allowed and in which combinations. XML schemas are an alternative to document type definitions (DTDs) and can be used to extend functionality in the areas of data typing, inheritance, and presentation.

Additional product information

The following additional resources are available online.

WebSphere Portal

- WebSphere Portal product support page: http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal
- WebSphere Portal information library: <http://www.ibm.com/software/genservers/portal/library/>
- WebSphere Portal wiki: <http://www.lotus.com/ldd/portalwiki.nsf>

WebSphere Application Server

- WebSphere Application Server product support page: <http://www.ibm.com/software/webservers/appserv/was/support/>
- WebSphere Application Server information library: <http://www.ibm.com/software/webservers/appserv/was/library/index.html>
- WebSphere Application Server 7.0.x information center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

Information centers

- Cognos Business Intelligence information center: <http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp>
- DB2 information center: <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp>

- IBM ILOG CPLEX Optimization Studio information center: <http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp>
- Lotus Domino information center: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Lotus Notes information center: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Lotus Sametime Standard information center: <http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp>
- Rational Application Developer information center: http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html
- Tivoli Access Manager information center: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Tivoli Composite Application Manager information center: <http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp>
- Tivoli Directory Integrator information center: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc_7.1/welcome.htm
- Tivoli Directory Server information center: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Tivoli Identity Manager information center: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Tivoli Netcool/Impact information center: <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html>
- Tivoli Netcool/OMNIbus information center: http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIbus.doc_7.3.1/omnibus/wip/welcome.htm
- Tivoli Service Request Manager information center: http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm
- IBM WebSphere Business Monitor information center: <http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html>
- WebSphere Message Broker information center: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp>
- WebSphere MQ information center: <http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp>
- WebSphere Operational Decision Management information center: <http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp>

Redbooks

- Redbooks Domain: <http://www.redbooks.ibm.com/>

Other web resources

- Tivoli training and certification: <http://www.ibm.com/software/tivoli/education/>
- OASIS Common Alerting Protocol Version 1.2 <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- Red Hat website: <http://www.redhat.com/>

Related concepts:

“Intended audience” on page 1

This product documentation is intended for people who are using, installing, administering, and maintaining the IBM Intelligent Operations Center. It also contains implementation documentation for customizing the solution and integrating the external underlying systems that IBM Intelligent Operations Center requires.

Copyright notice and trademarks

Copyright notice

© Copyright IBM Corporation 2011, 2012. All rights reserved. May only be used pursuant to an IBM software license agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished “as is” without warranty of any kind. **All warranties on this document are hereby disclaimed, including the warranty of non-infringement and the implied warranties of merchantability and fitness for a particular purpose.**

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

Trademarks

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities, and Redbooks are trademarks of the IBM Corporation in the United States, other countries, or both.

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

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries

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

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

Oracle, Javascript, and Java are registered trademarks of Oracle and/or its affiliates.

ArcGIS, EDN, StreetMap, @esri.com, and www.esri.com are trademarks, registered trademarks, or service marks of Esri in the United States, the European Community, or certain other jurisdictions.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities, and Redbooks are trademarks of the IBM Corporation in the United States, other countries, or both.

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

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries

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

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

Oracle, Javascript, and Java are registered trademarks of Oracle and/or its affiliates.

ArcGIS, EDN, StreetMap, @esri.com, and www.esri.com are trademarks, registered trademarks, or service marks of Esri in the United States, the European Community, or certain other jurisdictions.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Index

G

glossary 328

N

new features
 overview 8
notices 339

T

trademarks 339

Readers' Comments — We'd Like to Hear from You

IBM Intelligent Operations Center
IBM Intelligent Operations Center
Product Documentation
Version 1 Release 5

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 1-800-227-5088 (US and Canada)

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

Email address



Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM
Information Development Department DLUA
P.O. Box 12195
Research Triangle Park, NC
USA 27709-9990



Fold and Tape

Please do not staple

Fold and Tape



Printed in USA