

IBM Intelligent Operations Center
Version 1 Release 6

*Installing and Configuring IBM
Intelligent Operations Center for
Emergency Management*

IBM

IBM Intelligent Operations Center
Version 1 Release 6

*Installing and Configuring IBM
Intelligent Operations Center for
Emergency Management*

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 11.

This edition applies to IBM Intelligent Operations Center for Emergency Management version 1, release 6, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2015.**

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

Contents

Chapter 1. Installing and configuring the emergency management server and client 1
Installing the emergency management server . . . 1
Configuring signed security certificates 2
Configuring single sign-on. 3
Installing the emergency management client. . . . 4
Configuring missions to KPIs forwarding. 4

Chapter 2. Installing and configuring IBM Intelligent Operations Center for Emergency Management 7
Installing IBM Intelligent Operations Center for Emergency Management 7

Configuring alert forwarding 8

Appendix. License usage metrics. 9

Notices 11

Trademarks. 15

Chapter 1. Installing and configuring the emergency management server and client

Before you install IBM® Intelligent Operations Center for Emergency Management, install the emergency management server and client and configure single sign-on.

Installing the emergency management server

Install the emergency management server by using a provided control script file.

Before you begin

Before you install the emergency management server, ensure that the required minimal operating system is installed. IBM Intelligent Operations Center for Emergency Management version 1.6 supports Red Hat Enterprise Linux version 6.5. If you need to use Red Hat version 6.6 for security reasons, first install Red Hat kernel version 2.6.32-573.7.1.el6.x86_64 or later. Otherwise, IBM Intelligent Operations Center for Emergency Management might fail to install or to work. For more information about Red Hat updates, see <https://access.redhat.com/articles/3078>.

You must also have the emergency management server license file. If you do not have the license file, contact your IBM representative.

Ensure that the `/etc/hosts` file includes IP addresses for all IBM Intelligent Operations Center servers.

Procedure

To install the emergency management server:

1. Create the `/root/taccs_install` directory and copy the emergency management server control script `taccs_ctl` file to the new directory.
2. Configure the server to bootstrap by running the following command:

```
./taccs_ctl bootstrap
```

Running the bootstrap command configures a firewall, installs the Docker container manager, creates an optional administrator user account, and restarts all modified services.

3. Copy the emergency management server image `CN60YEN.iso` to the `/root/taccs_install` directory, and change directory to that directory.
4. Extract the image archive and load it into Docker on the server by running the following command as the root user:

```
./taccs_ctl load_image --archive-file=image_archive_file_name
```

For example: `./taccs_ctl load_image --archive-file=ibm-x64-5.0.1-release.docker.xz`

5. Run the setup configuration package as the `p5admin` user. The `p5admin` user was created during bootstrap configuration.
 - a. Create a `/p5data` directory that is owned by the `p5admin` user by running the following commands:

```
# mkdir /p5data
# chown -R p5admin:p5admin /p5data
```

- b. Locate the image file by running the Docker **images** command. For example,

```
# docker images
REPOSITORY          TAG          IMAGE ID        CREATED        VIRTUAL SIZE
quay.io/priority5/taccs_ibm  ibm-x64-5.0.1-release  f736ffee72d2  2 weeks ago  1.164 GB
```

- c. Load the sample configuration by running the following commands with the `REPOSITORY` and `TAG` values that are returned in the previous step:

```
# su - p5admin
./taccs_ctl sample_config --image=REPOSITORY_path:TAG --config-dir=/home/p5admin/deploy_5.0
chown -R p5admin:p5admin /home/p5admin/deploy_5.0
```

For example,

```
./taccs_ctl sample_config --image=quay.io/priority5/taccs_ibm:ibm-x64-5.0.1-release
--config-dir=/home/p5admin/deploy_5.0
chown -R p5admin:p5admin /home/p5admin/deploy_5.0
```

- d. As the `p5admin` user, set the values for the base settings that are needed to run the server by running the following commands:

```
su - p5admin
cd /home/p5admin/deploy_5.0
./taccs_ctl setup --host-data-dir=host_data_directory
--db-username=db_user --db-password=db_password
--ext-hostname=external_hostname
```

For example,

```
$ cd /home/p5admin/deploy_5.0
$ ./taccs_ctl setup --host-data-dir=/p5data --db-username=p5 --db-password=db_password
--ext-hostname=host.example.com
```

- e. Copy the license file to the configuration directory. For example, copy the license file `taccs_license.json` to the `/home/p5admin/deploy_5.0/config/taccs_es/` directory. You can rename the `taccs_license.json` file, but be sure to update the `/home/p5admin/deploy_5.0/config/taccs_es/base.conf.in` configuration file with the new file name.

Ensure that the license file is owned by the `p5admin` user.

- f. Verify that you can run the `taccs_ctl` control script file from the configuration directory by running the following command:

```
$ cd /home/p5admin/deploy_5.0
./taccs_ctl update
```

6. Initialize the database cluster that stores local application data by running the following command:

```
./taccs_ctl init_db. For example,
$ cd /home/p5admin/deploy_5.0
[p5admin@xyznn deploy_5.0]$ ./taccs_ctl init_db
```

7. Start the emergency management server by running the following command: `./taccs_ctl start`. For example,

```
$ cd /home/p5admin/deploy_5.0
[p5admin@xyznnn deploy_5.0]$ ./taccs_ctl start
```

This command starts each of the required containers and checks their status as they start. View the output from the command to see that start is proceeding and for details of any issues.

8. Check the status of the server by running the following command: `./taccs_ctl status`.

Configuring signed security certificates

To further ensure security, configure security certificates and update the emergency management server with IBM Intelligent Operations Center certificates.

Procedure

To configure security certificates:

1. Log on to the emergency management server as the `p5admin` user.
2. Copy your signed security certificates to the `/home/p5admin/deploy_5.0/config/ssl` directory on the emergency management server.

3. Back up the `/home/p5admin/deploy_5.0/deployment_config.py` file, then modify the original file to include the new security certificate file name in the following parameters:

```
server_pem_path = '/config_repo/site/ssl/emergency_management_server_host_name.pem'  
pg_cert_file = '/config_repo/site/ssl/emergency_management_server_host_name.crt'  
pg_key_file = '/config_repo/site/ssl/emergency_management_server_host_name.key'
```

4. Stop and restart the emergency management server by running the following commands:

```
p5admin> cd /home/p5admin/deploy_5.0  
p5admin> ./taccs_ctl stop  
p5admin> ./taccs_ctl start
```

Configuring single sign-on

Before you install and configure IBM Intelligent Operations Center for Emergency Management, configure single sign-on with the IBM Intelligent Operations Center LDAP server.

About this task

After the emergency management server is installed, configure single sign-on by modifying files on the emergency management server.

Procedure

To configure single sign-on (SSO):

1. Ensure that the emergency management server and the IBM Intelligent Operations Center server are in the same domain. If the emergency management server is on a different domain, add the emergency management server domain name in **Global Security > Web and SIP security > Single sign-on (SSO)** in the WebSphere® Application Server Deployment Manager console. Separate multiple domain names with a semi-colon (;).
2. Increase the **LTPA timeout** value to 500 minutes in **Global Security > LTPA** in the WebSphere Application Server Deployment Manager console. Restart the web server and portal.
3. Modify the `/home/p5admin/deploy_5.0/config/taccs_es/base.conf.in` file as the p5admin user.
 - a. Add the following code after the line `<usage_service enabled="false"/>`:

```
<rest_service>  
  <access_control method="ioc_ltpa2">  
    <default_data_group>{{default_data_group}}</default_data_group>  
    <url>https://IOC_web_server_host_name/ibm/ioc/api</url>  
  </access_control>  
</rest_service>
```

Important: Replace `IOC_web_server_host_name` with the host name for your IBM HTTP Server.

4. Start the emergency management server by running the following commands:

```
su p5admin  
cd /home/p5admin/deploy_5.0/  
./taccs_ctl stop  
./taccs_ctl start
```

5. Verify that you can log on with single sign-on.
 - a. Log on to IBM Intelligent Operations Center as the wpsadmin user.
 - b. Log on to the emergency management server with the following URL: `https://IOC_Emergency_Management_server_address/mobile/index.html`.
 - c. Log on to the emergency management server administration interface with the following URL: `https://IOC_Emergency_Management_server_address/web/admin.html#/user`.

Note: After IBM Intelligent Operations Center for Emergency Management is installed, the corresponding login URLs are:

- https://IOC_web_server_address/mobile/index.html
- https://IOC_web_server_address/web/admin.html#/user

Installing the emergency management client

After you configure single sign-on, install and configure the emergency management client.

Before you begin

The emergency management client runs only on a physical computer that runs Microsoft Windows. Virtual machines are not supported.

Procedure

To install the emergency management client:

1. Download the emergency management client installation program from the following URL: https://IOC_web_server_address/web/client_install.html. The installation program runs automatically on download.
2. Respond to the prompts from the installation program.
3. Start the emergency management client by running the C:\p5\TACCS\taccs\apps\dve\taccs_dve.exe file.
4. Copy the **Machine ID** value when it is displayed. The machine ID is required to grant the emergency management client access to the emergency management server.
5. Log on to the emergency management server as the p5admin user.
6. Change directory to /home/p5admin/deploy_5.0/config/dve.
7. Copy any existing directory to a directory named with the machine ID captured in step 4. For example:

```
[p5admin@xyznn ~]$ cp -Rp
    client_IDXXX-XXXX-XXXXXX-XXXXXXX new_user_name_9be31381-51e2-11cb-99e4-f66b7594f4b3
[p5admin@xyznn dve]$ ls -la new_user_name_9be31381-51e2-11cb-99e4-f66b7594f4b3
total 12
drwxr-xr-x  2 p5admin p5admin 4096 Nov  7 16:14 .
drwxr-xr-x 11 p5admin p5admin 4096 Nov  7 16:14 ..
-rw-r--r--  1 p5admin p5admin 40 Nov  7 16:14 machine.conf
[p5admin@xyznn dve]$ cat new_user_name_9be31381-51e2-11cb-99e4-f66b7594f4b3/machine.conf
```

```
<?xml version="1.0" ?>
<taccs>
  <!-- This is a place holder for machine specific configurations. All
    configurations specific to a machine would go into this file which
    is downloaded when the application is started. -->
</taccs>
```

8. Restart the emergency management server by running the following commands:

```
su - p5admin
cd /home/p5admin/deploy_5.0
./taccs_ctl stop
./taccs_ctl start
```

Configuring missions to KPIs forwarding

Configure communication between emergency management missions and IBM Intelligent Operations Center KPIs.

About this task

Missions in IBM Intelligent Operations Center for Emergency Management correspond to KPIs in IBM Intelligent Operations Center. You can configure communication between missions and KPIs.

Important: To ensure that all child rules are correctly mapped to the KPI Dashboard, create new missions instead of cloning existing missions.

Procedure

To configure missions to KPIs forwarding:

1. Configure the emergency management server with an encrypted API key for the wsadmin user ID. To obtain an API token and generate an encrypted API key:
 - a. Log on to the emergency management administrator console. For example, `https://emergency_management_server.example.com/web/admin.html`.
 - b. Click **wpsadmin > API Token**.
 - c. Copy the API key.
 - d. Using SSH, log on to the emergency management server as the p5admin user and encode the key. For example, run the following commands:

```
[p5admin@xyznn deploy_5.0]$ cd /home/p5admin/deploy_5.0
[p5admin@xyznn deploy_5.0]$ ./taccs_ctl encode API_encryption_key
ENC:encoded_API_encryption_key
```
2. Add the following text to the end of the `/home/p5admin/deploy_5.0/config/taccs_es/base.conf.in` file, before the `</taccs>` element:

```
<!-- KPI PUSH -->
<!-- Configuration for the Intelligent Operation Center worker.
see plugins/ibm/share/config/ibm_es.conf
NOTE: We cannot use host names that are in /etc/hosts on the host machine.
-->
<ibm>
<ioc_worker enabled="True" refresh_rate="100.0" mission_unity_tag="live_state">
  <data_group_id>{{default_data_group}}</data_group_id>
  <kpi enabled="False"/>
  <message_hook api_key="ENC:encoded_API_encryption_key">
    https://web_server.example.com/ibm/ioc/api/publicsafety/notification/taccs
  </message_hook>
</ioc_worker>
</ibm>
```

Update the web server host name and API for your environment.

3. Add the following text to the end of the `/home/p5admin/deploy_5.0/config/dve/base/base.conf.in` file, before the closing `</taccs>` element:

```
<!-- KPI Config - url: The url for the IOC api. Ex: https://<hostname>/ibm/ioc/api/
-->
<ioc url="https://<IOC_web_server>.example.com/ibm/ioc/api"/>
```

4. Stop and start the emergency management server by running the following commands:

```
su - p5admin
cd /home/p5admin/deploy_5.0
./taccs_ctl stop
./taccs_ctl start
```

Command results are written to the `/p5data/taccs/log/taccs_es_worker_01.log` file.

5. To refresh the KPI to missions, run an HTTP get command on the following URL:
`https://IOC_server/ibm/ioc/api/publicsafety/taccs-service/taccs/kpi/createKpiHierarchy`

Chapter 2. Installing and configuring IBM Intelligent Operations Center for Emergency Management

After you install and configure the emergency management server and client, install and configure IBM Intelligent Operations Center for Emergency Management V1.6 to work with the base installation of IBM Intelligent Operations Center and with your data sources.

Installing IBM Intelligent Operations Center for Emergency Management

After you ensure that prerequisites are in place, install IBM Intelligent Operations Center for Emergency Management.

Before you begin

You must already have IBM Intelligent Operations Center V1.6.0.3 Fix Pack PO03764, or later, installed and running before you install IBM Intelligent Operations Center for Emergency Management. See the documentation for *IBM Intelligent Operations Center 1.6.0.3 full installer* at <http://www.ibm.com/support/docview.wss?uid=swg24039491> for instructions on downloading and installing the required software.

Ensure that the `/etc/hosts` file includes the emergency management server IP addresses.

Procedure

To install IBM Intelligent Operations Center for Emergency Management:

1. Copy the `IBMIOC-Linux-EmergencyManagement.zip` file into the maintenance directory of the APAR Installer Framework. For example, copy the compressed file to `/installHome/ioc16/tools/aparInstaller/maintenance` or `/opt/ibm/IOC16install/ioc16/tools/aparInstaller/maintenance`.
2. Update the `iop.std.properties` file with the following properties:

```
TACCS.1.HOST
TACCS.1.ACCOUNT
TACCS.1.ACCOUNT.PWD
TACCS.1.SSH_PORT
```

3. Run the APAR installer by running the following commands:

```
cd /opt/ibm/IOC16install/ioc16/tools/aparInstaller
IOC_PCT_PASSWORD=IOC_control_password
./update.sh -f /opt/ibm/IOCInstall/ioc16/topology/iop.std.properties -t std
-m /distributionMedia/ -p topology_password
```

Note: The value for `IOC_control_password` is the IOCCControl password, which is typically the same as the topology password.

4. Update the system properties to point to the emergency management server.
 - a. To ensure that your browser has a valid cookie that includes an LTPA token to authenticate with the emergency management server, log on to IBM Intelligent Operations Center as the `wpsadmin` user.
 - b. Log on to the emergency management server at `https://IBM_HTTP_Server_address/web/admin.html`.
 - c. Click **wpsadmin > API Token** and copy the API key.
 - d. Log on to IBM Intelligent Operations Center and go to the Solution Administration view.
 - e. Select **System Properties**.

- f. Update the following system properties to match your system:

taccsHost

The value is typically the IBM HTTP Server host name.

taccsApiKey

The value is the API key that you copied in step 4.c.

5. Stop and restart the WebSphere Portal cluster by using the `IOCControl` command.
6. Tune the KPI refresh interval frequency, which is controlled by the system property `KpiReadRefreshRate`. The default refresh interval is 30 minutes.

Results

After IBM Intelligent Operations Center for Emergency Management is installed, the login URLs are:

- IBM Intelligent Operations Center for Emergency Management user: `https://IOC_web_server_address/mobile/index.html`
- IBM Intelligent Operations Center for Emergency Management administrator: `https://IOC_web_server_address/web/admin.html#/user`

Configuring alert forwarding

You can configure IBM Intelligent Operations Center alerts to be displayed in IBM Intelligent Operations Center for Emergency Management.

Procedure

1. Log on to IBM Intelligent Operations Center and go to Solution Administration view.
2. Create a data source.
3. Map the new data source to alert properties in the emergency management server.
 - The data source name is the source of the alert (**From**)
 - The property that is mapped to the minimal property **Name** is the alert title.
 - The following target properties map to alert specific columns:
 - `alert_description`
 - `alert_author`
 - `alert_address`
 - `alert_priority` (must be a number)
4. Select **Emergency Management > Data Forwarder**, click **Create**, and select **Data Source**, **Alert Type**, and **Data Group**.

Appendix. License usage metrics

IBM License Metric Tool helps Passport Advantage® clients determine their full and sub-capacity PVU licensing requirements.

Learn more: [IBM License Metric Tool](#).

The IBM Intelligent Operations Center for Emergency Management installer adds a product-specific tag file for the authorized user metric.

Usage information is written to Software License Metric Tag (SLMTag) files using a script provided with IBM Intelligent Operations Center for Emergency Management. These files have the extension `.slmtag` and are read periodically by the IBM License Metric Tool (ILMT) after it has been configured to scan for these files. You can generate reports that summarize usage.

For more information on using IBM License Management Tool, see the [IBM License Management Tool 9.0 Knowledge Center](#).

SLMTag logging

Each time IBM Intelligent Operations Center for Emergency Management starts, license management information is logged to the `/opt/IBM/ioc/properties/slmtags` directory. The logged `.slmtag` file contains usage information in the following format:

```
<Metric logTime="2015-05-28T11:25:46-04:00">
  <Type>APPLICATION</Type>
  <SubType></SubType>
  <Value>1</Value>
  <Period>
    <StartTime>2015-05-28T11:25:46-04:00</StartTime>
    <EndTime>2015-05-28T11:25:46-04:00</EndTime>
  </Period>
</Metric>
```

Notices

Product legal notices for IBM Intelligent Operations Center for Emergency Management V1.6.

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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 actual people or business enterprises is entirely coincidental.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright notice

© Copyright IBM Corporation 2015. 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, ibm.com[®], DB2[®], Domino[®], GDDM, ILOG[®], Lotus[®], Notes[®], Passport Advantage, Rational[®], Sametime[®], Tivoli[®], Service Request Manager[®], Smarter Cities[®], SPSS[®], Redbooks[®], WebSphere, and Worklight[®], 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.

Intel and Pentium are trademarks or registered trademarks 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, JavaBeans, and Java[™] are registered trademarks of Oracle and/or its affiliates.

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

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Readers' Comments — We'd Like to Hear from You

IBM Intelligent Operations Center
Installing and Configuring IBM Intelligent Operations Center for Emergency Management
Version 1 Release 6

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



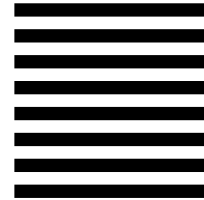
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

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



Product Number:

Printed in USA