

*InCharge*TM

Application Services Manager Deployment Guide

Version 5.0.1



Copyright ©1996-2002 by System Management ARTS Incorporated. All rights reserved.

The Software and all intellectual property rights related thereto constitute trade secrets and proprietary data of SMARTS and any third party from whom SMARTS has received marketing rights, and nothing herein shall be construed to convey any title or ownership rights to you. Your right to copy the software and this documentation is limited by law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Use of the software is governed by its accompanying license agreement. The documentation is provided "as is" without warranty of any kind. In no event shall System Management ARTS Incorporated ("SMARTS") be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, arising from any error in this documentation.

The InCharge products mentioned in this document are covered by pending patent applications and one or more of the following U.S. patents: 5,528,516 and 5,661,668 and 6,249,755.

"InCharge," the InCharge logo, "SMARTS," the SMARTS logo, "Graphical Visualization," "Authentic Problem," "Codebook Correlation Technology," and "Instant Results Technology" are trademarks or registered trademarks of System Management ARTS Incorporated. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Third-Party Software. The Software may include software of third parties from whom SMARTS has received marketing rights and is subject to some or all of the following additional terms and conditions:

Bundled Software

Sun Microsystems, Inc., Java(TM) Interface Classes, Java API for XML Parsing, Version 1.1. "Java" and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. SMARTS is independent of Sun Microsystems, Inc.

W3C IPR Software

Copyright © 2001-2002 World Wide Web Consortium (<http://www.w3.org>), (Massachusetts Institute of Technology (<http://www.lcs.mit.edu>), Institut National de Recherche en Informatique et en Automatique (<http://www.inria.fr>), Keio University (<http://www.keio.ac.jp>)). All rights reserved (<http://www.w3.org/Consortium/Legal/>). Note: The original version of the W3C Software Copyright Notice and License can be found at <http://www.w3.org/Consortium/Legal/copyright-software-19980720>.

The Apache Software License, Version 1.1

Copyright ©1999-2002 The Apache Software Foundation. All rights reserved. Redistribution and use of Apache source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of Apache source code must retain the above copyright notice, this list of conditions and the Apache disclaimer as written below.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the Apache disclaimer as written below in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:
"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "The Jakarta Project", "Tomcat", "Xalan" and "Apache Software Foundation" must not be used to endorse or promote products derived from Apache software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this Apache software may not be called "Apache," nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

APACHE DISCLAIMER: THIS APACHE SOFTWARE FOUNDATION SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA, OR PROFITS, OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Apache software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright © 1999, Lotus Development Corporation., <http://www.lotus.com>. For information on the Apache Software Foundation, please see <http://www.apache.org>.

FLEXIm Software

© 1994 - 2002, GLOBEtrotter Software Inc. All rights reserved. "GLOBEtrotter" and "FLEXIm" are registered trademarks of GLOBEtrotter Software Inc. For product and legal information, see <http://www.globetrotter.com/manual.htm>.

ptmalloc Software

© 1997 - 2002 Wolfram Gloger. All rights reserved. PERMITTED USES. Permission to use, copy, modify, distribute, and sell the ptmalloc software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notice and this permission notice appear in all copies of the Software and related documentation, and (ii) the name of Wolfram Gloger may not be used in any advertising or publicity relating to the Software.

LIMITATION OF LIABILITY. THE PTMALLOC SOFTWARE IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL WOLFRAM GLOGER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE SMARTS SOFTWARE.

JfreeChart – Java library for GIF generation

The Software is a "work that uses the library" as defined in GNU Lesser General Public License Version 2.1, February 1999 Copyright © 1991, 1999 Free Software Foundation, Inc., and is provided "AS IS" WITHOUT WARRANTY OF ANY KIND EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED IN THE ABOVE-REFERENCED LICENSE BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. JfreeChart library (included herein as .jar files) is provided in accordance with, and its use is covered by the GNU Lesser General Public License Version 2.1, which is set forth at <http://www.object-refinery.com/lgpl.html/>.

BMC – product library

The Software contains technology (product library or libraries) owned by BMC Software, Inc. ("BMC Technology"). BMC Software, Inc., its affiliates and licensors (including SMARTS) hereby disclaim all representations, warranties and liability for the BMC Technology.

Crystal Decisions Products

The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 ("Crystal Decisions"). All such software products are the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS' TECHNOLOGY, TO SMARTS FOR A FULL REFUND, OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU Cygwin utilities

Cygwin utilities are used by the Software's install and uninstall programs. The Cygwin utilities are resident on the CD on which the Software was delivered to you, and are installed to the host machine. The Cygwin utilities software program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version. The full text of the applicable GNU GPL is available for viewing at <http://www.cygwin.com/COPYING>. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The Cygwin utilities program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU Cygwin utilities provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

GNU eTeks PJA Toolkit

Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.

The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEKS' web site: <http://www.eteks.com>. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation, version 2 of the License. The full text of the applicable GNU GPL is available for viewing at <http://www.gnu.org/copyleft/gpl.txt>. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX

The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform

The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: <http://www.hp.com>. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies

Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

Contents

Preface	vii
Intended Audience	vii
Prerequisites	viii
Document Organization	viii
Documentation Conventions	viii
Additional Resources	ix
InCharge Commands	ix
Documentation	ix
Common Abbreviations and Acronyms	xi
Technical Support	xi
1 Overview of InCharge Application Services Manager	1
Architecture of Application Services Manager	1
Topology and Events for Application Services Manager	3
Discovering Topology	3
Naming Topology Elements	5
Mapping Events to Application Services Manager Symptoms	5
2 Deploying InCharge Application Services Manager	7
Deploying InCharge Adapter for BMC Patrol	8
Deploying InCharge Adapter for Concord SystemEDGE	9
Deploying InCharge Adapter for Concord SystemEDGE with the InCharge SNMP Trap Adapter	9
Deploying the InCharge Adapter for Concord SystemEDGE	10
Deploying the Global Manager	11
Deploying Application Services Manager	12
Description of the asm.conf Configuration File	12

Index

17

Preface

This document describes how to deploy InCharge Application Services Manager (Application Services Manager). It supplements the deployment information contained in the *InCharge Service Assurance Manager Configuration Guide* by providing information specific to Application Services Manager.

As such, it describes the steps necessary to configure all of the components involved in an Application Services Manager deployment:

- InCharge SMART Adapters, including the InCharge Adapter for BMC Patrol and InCharge Adapter for Concord SystemEDGE
- Global Manager
- Application Services Manager

Except for Application Services Manager, the detailed configuration information necessary to complete deployment is available in the user or configuration guides provided with that product.

Intended Audience

This document is intended for the person responsible for deploying Application Services Manager. It may also be of interest to those who want to understand the architecture and operation of Application Services Manager.

Prerequisites

InCharge Service Assurance Manager (Service Assurance) should already be installed, configured, and operational. In addition, the person deploying Application Services Manager should be familiar with the deployment of Service Assurance and have the authority to configure Service Assurance as necessary to deploy Application Services Manager.

Document Organization

This guide consists of the following sections:

1. OVERVIEW OF INCHARGE APPLICATION SERVICES MANAGER	Describes the components of Application Services Manager and the data it requires to perform analysis.
2. DEPLOYING INCHARGE APPLICATION SERVICES MANAGER	Describes the steps necessary to deploy or configure the components of Application Services Manager and Service Assurance.

Table 1: Document Organization

Documentation Conventions

Several conventions may be used in this document as shown in Table 2.

CONVENTION	EXPLANATION
<code>sample code</code>	Indicates code fragments and examples in Courier font
keyword	Indicates commands, keywords, literals, and operators in bold
<code>%</code>	Indicates C shell prompt
<code>#</code>	Indicates C shell superuser prompt
<code><parameter></code>	Indicates a user-supplied value or a list of non-terminal items in angle brackets
<code>[option]</code>	Indicates optional terms in brackets

CONVENTION	EXPLANATION
<i>/InCharge</i>	Indicates directory path names in italics
yourDomain	Indicates a user-specific or user-supplied value in bold, italics
<i>File > Open</i>	Indicates a menu path in italics
▲ ▼	Indicates a command that is formatted so that it wraps over one or more lines. The command must be typed as one line.

Table 2: Documentation Conventions

In this document, the term **BASEDIR** represents the location where InCharge software is installed. The term **BASEDIR** represents the */opt/InCharge<n>* directory for UNIX, the *C:\InCharge<n>* directory for Windows (where <n> represents the InCharge software version number), or your specified path. The InCharge software resides in the **BASEDIR**/*smarts* subdirectory.

Directory path names are shown with forward slashes (/). Users of the Windows operating systems should substitute back slashes (\) for forward slashes.

Also, if there are figures illustrating consoles in this document, they represent the consoles as they appear in Windows. Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, a plus sign displays for Windows and an open circle displays for UNIX.

Additional Resources

In addition to this manual, SMARTS provides the following resources.

InCharge Commands

Descriptions of InCharge commands are available as HTML pages. The *index.html* file, which provides an index to the various commands, is located in the **BASEDIR**/*smarts/doc/html/usage* directory.

Documentation

Readers of this manual may find other SMARTS documentation (also available in the **BASEDIR**/*smarts/doc/pdf* directory) helpful.

InCharge Documentation

The following SMARTS documents are product independent and thus relevant to users of all InCharge products:

- *InCharge Release Notes*
- *InCharge Documentation Roadmap*
- *InCharge Installation Guide*
- *InCharge System Administration Guide*
- *InCharge Notification Adapters User's Guide*

InCharge Service Assurance Manager Documentation

The following SMARTS documents are relevant to users of InCharge Service Assurance Manager:

- *An Introduction to InCharge Service Assurance Manager*
- *InCharge Service Assurance Manager Operator's Guide*
- *InCharge Service Assurance Manager Configuration Guide*
- *InCharge Service Assurance Manager Open Integration Configuration Guide*
- *InCharge Service Assurance Manager Failover System User's Guide*
- *InCharge Service Assurance Manager User's Guide for Business Impact Manager*
- *InCharge Service Assurance Manager User's Guide for Report Manager*
- *InCharge Service Assurance Manager Web Portal Operator's Guide*
- *InCharge Service Assurance Manager Web Portal Configuration Guide*

InCharge Application Services Manager Documentation

The following SMARTS documents are relevant to users of InCharge Application Services Manager:

- *InCharge Application Services Manager Deployment Guide*
- *InCharge Application Services Manager User's Guide*
- *InCharge Application Services Manager SMART Adapters User's Guide*

Common Abbreviations and Acronyms

The following lists common abbreviations and acronyms that are used in the InCharge guides.

ASL	Adapter Scripting Language
CDP	Cisco Discovery Protocol
ICIM	InCharge Information Model
ICMP	Internet Control Message Protocol
IDS	Incremental Device Support
IP	Internet Protocol
MIB	Management Information Base
MODEL	Managed Object Definition Language
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

Technical Support

SMARTS provides technical support by e-mail or phone during normal business hours (9:00 A.M. - 6:00 P.M. U.S. Eastern Time).

TECHNICAL SUPPORT: *support@smarts.com*

SALES: *sales@smarts.com*

WORLD WIDE WEB: *http://www.smarts.com*

TELEPHONE: +1.914.948.6200

FAX: +1.914.948.6270

You may also contact us at:

SMARTS
44 South Broadway
White Plains, New York 10601 U.S.A

Overview of InCharge Application Services Manager

InCharge Application Services Manager (Application Services Manager) monitors the end-to-end delivery of application services, identifies authentic problems, and determines the impact of these problems on application services.

This chapter describes the architecture and components of an Application Services Manager deployment. It also describes the type of information required by Application Services Manager to perform its analysis. Understanding these requirements can help you to effectively deploy SMART Adapters.

Architecture of Application Services Manager

Application Services Manager is typically deployed as part of a system that includes InCharge Service Assurance Manager, InCharge IP Availability Manager, and one or more SMART Adapters. Figure 1 illustrates a typical deployment of Application Services Manager.

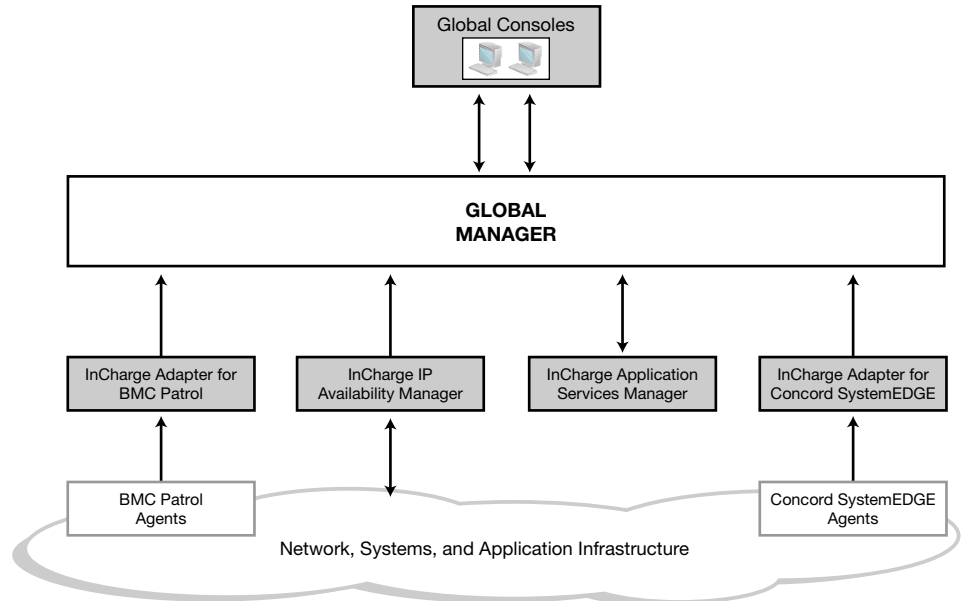


Figure 1: Architecture Of Application Services Manager Deployment

Figure 1 also shows the flow of information between the components of Application Services Manager and Service Assurance. A description of each component follows:

- InCharge Adapter for BMC Patrol discovers Patrol Agents, creates a topology of applications and the systems that host them, receives and processes events from the Patrol Agents, and passes this information to the Global Manager.
- InCharge Adapter for Concord SystemEDGE receives traps from SystemEDGE agents, creates topology, aggregates events, and passes this information to the Global Manager.
- InCharge IP Availability Manager discovers system elements and performs root-cause and impact analysis for LAN and WAN IP networks. The topology and analysis performed by Availability Manager is forwarded to the Global Manager.
- Global Manager consolidates topology and event information it receives from the SMART Adapters and Availability Manger. Application Services Manager imports the topology and event information from the Global Manager. The Global Manager also serves as the access point for operators who use the Global Console to monitor the managed systems.

- Application Services Manager analyzes the events and topology information to diagnose authentic problems in applications and application services. In addition, Application Services Manager determines the impact of authentic problems on the end-to-end application service delivery. The results of this analysis are sent to the Global Manager, where they can be viewed through the Global Console.
- Global Console displays the results of Application Services Manager's analysis in Notification Logs and Applications maps. Users with administrative privileges can also create topology through the Applications maps. For more information regarding this feature, see the *InCharge Service Assurance Manager Configuration Guide*.

Topology and Events for Application Services Manager

Application Services Manager correlates the events it receives from the Global Manager. As noted earlier, the InCharge Adapter for BMC Patrol and the InCharge Adapter for Concord SystemEDGE are two sources for these events.

When deploying SMART Adapters, you must ensure that the following occur:

- 1 Discovery of the applications and services topology.
- 2 Consistent naming of topology elements across all InCharge software.
- 3 Filtering and mapping of application and services events to the symptoms used by Application Services Manager for diagnosis.

Discovering Topology

For a complete analysis of possible problems and their impact, the managed topology should include the following elements:

- Hosts on which managed applications are running or hosts that provide services, such as DNS, on which applications or service delivery depend.
- Application services that represent the application task or service that is provided. Application services include application clusters, management agents, and applications.

- Transactions or sessions that indicate connections between applications. Sessions are persistent connections.

In addition, the topology can also include the components of host systems, such as processes, file systems, disks, swap area, memory, and processors. Events from these components are typically aggregated to a system-level event.

There are several methods for discovering this topology. Remember that the Global Manager consolidates topology and events and sends this information to the Application Services Manager for analysis.

- InCharge IP Availability Manager discovers the network elements over which the applications services are provided as well as the hosts on which the managed applications and services run. Availability Manager sends the topology and events to the Global Manager.
- InCharge Adapter for BMC Patrol can create the topology of hosts and applications. This can also be extended to discover system components such as processors and memory.
- InCharge Adapter for Concord SystemEDGE or the InCharge SNMP Trap Adapter can also create topology elements. When a trap is received from an SNMP agent, the trap adapter can be configured to automatically create the appropriate topological element and associate the event with it. For example, if an event regarding an application is received, the trap adapter can create an object for the application, an object for the host on which the application runs, and link them with the Hosts/HostedBy relationship.

When the InCharge SNMP Trap Adapter receives a trap from SiteScope, for example, it can create a transaction. In addition, the endpoints of the application service can also be created. If the endpoint application resides on a host, then the trap adapter associates each application endpoint with a host using the HostedBy relationship. The SiteScope application is related to the Transaction by the Consumes relationship, and the target application is related to it using the Produces relationship.

- Users with administrative privileges can use the Global Console to create instances of the ApplicationService, ApplicationCluster, MgmtService, and Application classes.

Naming Topology Elements

Because the Global Manager receives events from different sources, it is important that the affected elements are correctly identified and consistently named. To illustrate this point, consider a host discovered by InCharge IP Availability Manager is not responding to SNMP requests. This information is sent to the Global Manager. A management agent running on that host generates a trap that indicates that the processor is over utilized. A SMART Adapter receives this trap, associates it with the host, and sends it to the Global Manager. In order for the Global Manager to diagnose authentic problems from both network-related events and application-related events, the name of the host in this scenario should be the same.

To facilitate this process, you should establish a naming scheme and implement it across all SMART Adapters and any Open Integration servers. You can control naming by using an ASL script to enforce a naming convention in an Open Integration server.

You can control the naming of topology elements through the configuration file of a SMART Adapter. This is especially important when a SMART Adapter is configured to create topology elements.

Mapping Events to Application Services Manager Symptoms

Application Services Manager requires the topology and event information described in Table 1 to diagnose authentic problems and determine their impact. To provide event and topology information, you must map events from system and application agents to these symptoms.

Table 1 also appears in the *InCharge Application Services Manager SMART Adapter User's Guide* so that you can refer to it while configuring a SMART Adapter.

SYMPTOMATIC EVENT	SOURCE	DESCRIPTION
ApplicationService DegradedSymptom	Application agent	Indicates that the application or application cluster is not functioning as expected, but is not completely down. An aggregate of events that indicate performance problems with an application. For example, an application that is unable to open a connection because the thread pool on the system is exhausted.
ApplicationService DownSymptom	Application agent	Indicates that the application or application cluster is not functioning. An event or aggregate of events that indicate that the application is down.

SYMPTOMATIC EVENT	SOURCE	DESCRIPTION
UnitaryComputerSystem DegradedSymptom	System agent	Indicates that the system is experiencing problems that may affect applications hosted on the system. An aggregate of events that indicate problems on a system. Examples include high CPU utilization, low memory or page fault problems, full disk capacity or read/write errors.
UnitaryComputerSystem Unresponsive	InCharge IP Availability Manager	Indicates that the system is not reachable over the network. This event is automatically imported from InCharge IP Availability Manager and is used to explain Session, Transaction, and ApplicationConnection problems.
Session Disconnected	Session monitor	Indicates that a connection between application components is no longer established or has become disconnected. Map events that indicate a continuous communication session has ended unexpectedly.
Transaction TimedOut	Transaction monitor	Indicates that the transaction monitor did not receive a response to a transaction request. Map traps from page pullers or agents that provide information about transaction performance.
Transaction Slow	Transaction monitor	Indicates that the transaction monitor received a response for a transaction request but that the response took too long to complete. Map traps from page pullers or agents that provide information about transaction performance.
Transaction Errors	Transaction monitor	Indicates that the transaction monitor received a response but the response contained incorrect or unexpected data. Map traps from page pullers or agents that provide information about transaction performance.

Table 1: Symptomatic Events for Application Services Manager

Deploying InCharge Application Services Manager

InCharge Application Services Manager (Application Services Manager) also requires InCharge Service Assurance Manager (Service Assurance). This document concentrates on the deployment of Application Services Manager, assuming that Service Assurance is already deployed as described in the *InCharge Service Assurance Manager Configuration Guide*.

Deploying Application Services Manager involves configuring one or more of the following components:

- InCharge Adapter for BMC Patrol
- InCharge Adapter for Concord SystemEDGE
- Service Assurance Global Manager
- InCharge Application Services Manager

The general rule of thumb for deploying these components is to follow the flow of data. This means starting with the SMART Adapters, up to the Global Manager, then to the domain manager of Application Services Manager.

Deploying InCharge Adapter for BMC Patrol

The InCharge Adapter for BMC Patrol is capable of discovering Patrol Agents, processing and aggregating events from the agents, and creating the topology elements related to received events.

To deploy the adapter, perform the following steps:

- 1 Compile a list of BMC Patrol agents that the adapter should discover. For each agent, this list should include:
 - The host name or IP address of the system where the Patrol Agent is running. This name should be identical to the name used by InCharge IP Availability Manager.
 - The port number the Patrol Agent is listening on.
 - The username and password required to access the Patrol Agent.
- 2 Use *sm_edit* to make a local copy of *bmc.seedfile* in the **BASEDIR**/*smarts/local/conf/bmc* directory. Add the information you compiled to the *bmc_seedfile* file.
- 3 Edit a local copy of the *bmc.conf* file to ensure that the following settings are correct for your environment:
 - Review the *BMCDriverSection*. These parameters control communication between the adapter and the agents and can be used to filter events that you do not want the adapter to process.
 - If you intend to use the adapter to create applications and hosts topology, check that the *BMCTopoDump* section specifies the correct name of the applications to discover from the Patrol Agents.
- 4 Review the *bmc_events.conf* file to check the mapping of events sent by the Patrol Agent to symptoms used by Application Services Manager. If necessary, edit a local copy of the file to add additional events.
- 5 Start the adapter.

For more information regarding the configuration of the InCharge Adapter for BMC Patrol, see the *InCharge Application Services Manager SMART Adapter User's Guide*.

Deploying InCharge Adapter for Concord SystemEDGE

The InCharge Adapter for Concord SystemEDGE processes traps that it receives from Concord SystemEDGE agents. You can deploy the adapter using one of the following two methods:

- If you are running the InCharge SNMP Trap Adapter, you can add the trap information specific to the InCharge Adapter for Concord SystemEDGE to the trap configuration file of the InCharge SNMP Trap Adapter.
- If you are not running the InCharge SNMP Trap Adapter, you can run the InCharge Adapter for Concord SystemEDGE.

Deploying InCharge Adapter for Concord SystemEDGE with the InCharge SNMP Trap Adapter

The instructions below assume that an Open Integration server and the InCharge SNMP Trap Adapter are already configured and running. For information regarding the configuration of these components, see the *InCharge Service Assurance Manager Open Integration Configuration Guide*.

- 1 Use *sm_edit* to create a local copy of the *trap_mgr.conf* file that contains the trap definitions for Concord SystemEDGE agents. The original file is located in the **BASEDIR**/*smarts/conf/sysedge* directory.
- 2 Copy the trap definitions from the *trap_mgr.conf* file located in the **BASEDIR**/*smarts/local/conf/sysedge* directory and add them to the bottom of the *trap_mgr.conf* file located in the **BASEDIR**/*smarts/local/conf/icoi* directory.

This assumes that a local copy of *trap_mgr.conf* already resides in the **BASEDIR**/*smarts/local/conf/icoi* directory.

- 3 Edit the trap definitions for the Concord SystemEDGE agents to include any additional traps you want to map to Application Services Manager symptoms.
- 4 Configure the Concord SystemEDGE agents to send traps to the host where the InCharge SNMP Trap Adapter is running.
- 5 Stop and start the InCharge SNMP Trap Adapter.

Deploying the InCharge Adapter for Concord SystemEDGE

In a standalone deployment of the Concord SystemEDGE adapter, you must also install and configure an Open Integration server to receive traps from the adapter.

In addition, you can also use InCharge IP Availability Manager to discover the network and systems topology on which the application services run. The Open Integration server can import this topology and associate the traps it receives from the SystemEDGE agents with the correct topology element. For more information regarding the Topology Import feature of Open Integration, see the *InCharge Service Assurance Manager Open Integration Configuration Guide*.

The following steps assume that the Open Integration server is installed.

- 1 If a local copy of the Open Integration server's configuration file does not already exist, use *sm_edit* to create one. The original file is located in the **BASEDIR**/*smarts/conf/icoi* directory.
- 2 If you are using an InCharge IP Availability Manager as an underlying server, edit the local copy of *icoi.conf* to specify the name of the underlying domain.

If you are not running an underlying domain, edit the local copy of *icoi.conf* to comment out the *DomainType* section that defines an underlying domain.

- 3 Start, or restart, the Open Integration server.
- 4 Use *sm_edit* to create a local copy of the *trap_mgr.conf* file that contains the trap definitions for Concord SystemEDGE agents. The original file is located in the **BASEDIR**/*smarts/conf/sysedge* directory.
- 5 Edit the trap definitions for the Concord SystemEDGE agents to include any additional traps you want to map to Application Services Manager symptoms.
- 6 Configure the Concord SystemEDGE agents to send traps to the host where the InCharge SNMP Trap Adapter is running.
- 7 Use *sm_edit* to open a local copy of the *ic-trapd-receiver* startup script. A local copy is automatically installed into the **BASEDIR**/*smarts/local/script* directory. Check the values of the following variables and edit them as necessary:

- *DMNAME* should be set to the name of the InCharge SNMP Trap Adapter

- REMOTE_DMNAME should be set to the name of the Open Integration server
 - CONFDIR should be set to "sysedge"
- 8** Start the InCharge SNMP Trap Adapter using the *ic-trapd-receiver* startup script.

If you want to configure the trap adapter to start automatically, see the *InCharge System Administration Guide*.

Deploying the Global Manager

This deployment guide assumes that you have configured and deployed the Global Manager. However, you must make sure that the Global Manager's configuration file defines a DomainType section for the following components:

- InCharge Adapter for BMC Patrol
- Open Integration server
- Application Services Manager

For more information about the *ics.conf* configuration file, see the *InCharge Service Assurance Manager Configuration Guide*.

- 1** Use *sm_edit* to open the local copy of the *ics.conf* file.
- 2** By default, the *ics.conf* file includes DomainType definitions for both the InCharge Adapter for BMC Patrol and Application Services Manager. However, these DomainType definitions are commented out. Remove the comment marker from the DomainType definitions for INCHARGE-ASM and BMC-SA. In addition, check that the values of the Name fields match the names of the InCharge Adapter for BMC Patrol and Application Services Manager.
- 3** Add a DomainType definition for the Open Integration server you created above. In the ConfFile field, specify the *dxo-oi.conf* file.
- 4** Reconfigure the Global Manager.

Deploying Application Services Manager

Application Services Manager performs the analysis on the events and topology it receives from the Global Manager. In return, Application Services Manager sends the results of its analysis back to the Global Manager.

Because Global Manager provides topology and events to Application Services Manager, it functions as an underlying domain. This means that the configuration file for Application Services Manager, *asm.conf*, must include a DomainType definition for the Global Manager.

- 1 Use *sm_edit* to open a local copy of the *asm.conf* configuration file. The original file is located in the **BASEDIR**/*smarts/conf/asm* directory.
- 2 Verify that the DomainType section includes a definition for the Global Manager. The default name of the Global Manager is "INCHARGE-SA".

Description of the *asm.conf* Configuration File

The configuration file for Application Services Manager, *asm.conf*, uses the same syntax as the *ics.conf* file, which is described in the *InCharge Service Assurance Manager Configuration Guide*.

Unlike *ics.conf*, however, the *asm.conf* file only includes two sections:

- DomainSection, which specifies the Global Manager from which Application Services Manager receives events and topology.
- EventMappingSection, which translates the status of notifications received from the Global Manager to a status used by Application Services Manager.

The DomainType section is described in the *InCharge Service Assurance Manager Configuration Guide*. The following section describes the EventMappingSection, which is unique to Application Services Manager.

Description of the EventMappingSection

An EventMappingSection defines one or more EventMappingList subsections. Each EventMappingList subsection includes a name and includes one or more EventMap definitions. An EventMap translates the status of a notification attribute from the Global Manager, specified in the DomainType section, to attribute values used by Application Services Manager. Application Services Manager uses the translated values to perform its analysis.

Note: You should not edit this section of the *asm.conf* file.

An EventMap is comprised of six fields, as shown in the following example.

```
EventMap
{
    ClassName      = "UnitaryComputerSystem";
    EventName     = "Unresponsive";
    AttrName      = "OperationalState";
    ValueNotify   = "UNRESPONSIVE";
    ValueClear    = "RESPONSIVE";
    ValueUnknown  = "UNKNOWN_OPER_STATE";
}
```

Table 2 describes the fields of an EventMap section.

FIELD	DESCRIPTION
ClassName	Class name of the instance where the event occurred, including any subclasses and instances of those subclasses. Subclasses of UnitaryComputerSystem include: <ul style="list-style-type: none"> • Bridge • Host • Hub • Other • Probe • Repeater • Router • Server • Switch • TerminalServer
EventName	Name of the notification as received from the Global Manager.
AttrName	Name of the attribute used by Application Services Manager to which the values are mapped.
ValueNotify	Value of EventName when the notification is notified; meaning that the value of the EventState notification attribute is ACTIVE.

FIELD	DESCRIPTION
ValueClear	Value of EventName when the notification is cleared; meaning that the value of the EventState notification attribute is INACTIVE.
ValueUnknown	Value of EventName when the value of the notification is unknown; meaning that the value of the EventState notification attribute is either SUSPENDED or WAS_ACTIVE.

Table 2: EventMap Fields

Index

A

- Adapter
 - Deploying 3
 - InCharge Adapter for BMC Patrol 2, 4
 - Adding agents 8
 - bmc.conf 8
 - bmc.seedfile 8
 - bmc_events.conf 8
 - InCharge Adapter for Concord SystemEDGE 2, 4
 - ic-trapd-receiver 10
 - trap_mgr.conf 10
 - InCharge SNMP Trap Adapter 4, 9
 - trap_mgr.conf 9

Agents

- Adding to InCharge Adapter for BMC Patrol 8
- Application 5, 6
- System 6

Application class 4

Application services

- Discovering 3

Application Services Manager 3

- asm.conf 12
- Components 7
- Deploying 7

ApplicationCluster class 4

ApplicationService class 4

ApplicationService DegradedSymptom 5

ApplicationService DownSymptom 5

asm.conf 12

EventMap

- AttrName 13
- ClassName 13
- EventName 13
- ValueClear 14
- ValueNotify 13
- ValueUnknown 14

EventMappingList 12

Availability Manager 6

- Discovery 4

B

BASEDIR ix

bmc.conf 8

BMCDriverSection 8

BMCTopoDump 8

bmc.seedfile 8

bmc_events.conf 8

BMCDriverSection 8

BMCTopoDump 8

C

Class

- Application 4
- ApplicationCluster 4
- ApplicationService 4
- MgmtService 4

Configuration file

- asm.conf 12
- bmc.conf 8
- bmc.seedfile 8
- bmc_events.conf 8
- dxa-oi.conf 11
- icoi.conf 10
- ics.conf 11
- trap_mgr.conf 9, 10

Console 2, 3, 4

D

Deploying adapters 3

Deploying Application Services Manager 7

Discovering

- Application services 3
- Topology 4

Discovery

- Availability Manager 4

DomainType

- icoi.conf 10
- ics.conf 11
- dxa-oi.conf 11

E

Event

- ApplicationService DegradedSymptom 5
- ApplicationService DownSymptom 5
- Mapping 5

- Session Disconnected 6
- Transaction Errors 6
- Transaction Slow 6
- Transaction TimedOut 6
- UnitaryComputerSystem DegradedSymptom 6
- UnitaryComputerSystem Unresponsive 6
- Event sources 3
 - Application agents 5, 6
 - System agents 6
 - Transaction monitors 6
- EventMap 13

G

- Global Console 2, 3, 4
- Global Manager 2
 - ics.conf 11

H

- Hosts 3, 4

I

- icoi.conf 10
 - DomainType 10
- ics.conf 11
 - DomainType 11
- ic-trapd-receiver 10
 - CONFDIR 11
 - DMNAME 10
 - REMOTE_DMNAME 11
- InCharge Adapter for BMC Patrol
 - see Adapter
- InCharge Adapter for Concord SystemEDGE
 - see Adapter
- InCharge Application Services Manager
 - see Application Services Manager
- InCharge Console
 - see Global Console
- InCharge IP Availability Manager
 - see Availability Manager
- InCharge SNMP Trap Adapter
 - see Adapter

M

- MgmtService class 4

N

- Naming topology elements 5

O

- Open Integration
 - icoi.conf 10

S

- Script
 - ic-trapd-receiver 10
- Seed file
 - bmc.seedfile 8
- Session Disconnected 6
- Sessions 4
- SNMP trap 4
- Source of events 3
- System components 4

T

- Technical Support xi
- Topology
 - Application 4
 - ApplicationCluster 4
 - ApplicationService 4
 - Discovering 3, 4
 - Hosts 3, 4
 - MgmtService 4
 - Naming elements 5
 - Sessions 4
 - System components 4
 - Transactions 4
- Transaction Errors 6
- Transaction monitors 6
- Transaction Slow 6
- Transaction TimedOut 6
- Transactions 4
- Trap adapter 9
- trap_mgr.conf 9, 10

U

- UnitaryComputerSystem DegradedSymptom 6
- UnitaryComputerSystem Unresponsive 6