EMC® Smarts®
Service Assurance Manager

Version 9.2

Introduction

P/N 300-999-854
REV 01

EMC²

Copyright © 1996 - 2013 EMC Corporation. All rights reserved. Published in the USA.

Published March, 2013

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC^2, EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

CONTENTS

Preface

Chapter 1 Architectural Overview

Service Assurance Manager architecture 16
Service Assurance Manager 17
Global Console 17
Companion User Interface 17
Integration with third-party applications 18
Service Assurance Failover System 19
Service Assurance modules 19
EMC Smarts Business Impact Manager 19
EMC Smarts Web Console 20
EMC Smarts Business Dashboard 20

Chapter 2 Functional Overview

Service Assurance Manager features and functions 22
Automatic topology and event consolidation 22
Automatic topology abstraction 23
Global Console 23
Notification Log Console 24
Topology Browser Console 24
Map Console 25
Summary View Console 25
Status Table Console 25
Domain Manager Administration Console 26
Global Manager Administration Console 26
Service Assurance functions 27
Notification severity 27
Notification List 27
Tools 28
Notification escalation 28
Audit log 28
Containment 29
Security 29
Service Assurance module functions 31
EMC Smarts Business Impact Manager functions 31
EMC Smarts Business Dashboard functions 31

Chapter 3 Implementation Scenarios

Challenges of network management 34
EMC Smarts solutions 34
Fast and accurate fault isolation 34
Automated corrective actions 34
Business focus 34
Integration 35
Rapid deployment and low maintenance 35
Enterprise provider 36

Network service provider..... 38

Index

FIGURES

	Title	Page
1	EMC Smarts Service Assurance Manager architecture	16
2	Integration with third-party applications	18
3	Web Console and EMC Smarts Business Dashboard architecture	20
4	Difference between detailed and abstracted representation	23
5	Enterprise solution	37

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

NOTICE

This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website to ensure that you are using the latest version of this document.

Purpose

The Service Assurance Manager (Service Assurance) solution automatically correlates topology and event data from multiple EMC Smarts managed domains to diagnose root-cause problems and (with Business Impact Manager) the impact that those problems have on business-critical processes and services. EMC Smarts managed domains can include IP networks, systems, routing protocols, ATM/Frame Relay, applications, and business entities. Service Assurance Manager enables operations personnel to effectively prioritize their time and resources to maintain and sustain the business-critical processes and services.

EMC Smarts Service Assurance Manager Introduction provides high-level architectural and functional overviews of the EMC Smarts Service Assurance Manager solution. It also provides several examples of implementation scenarios.

Audience

This document is intended for operations staff, managers, and administrators who are interested in automated Service Assurance solutions.

EMC Smarts Service Assurance Manager installation directory

In this document, the term BASEDIR represents the location where EMC Smarts software is installed:

- For Windows, this location is: C:\InCharge*‹product›*.

On Windows operating systems, this product is, by default, installed to: C:\InCharge\SAM\smarts. This location is referred to as *BASEDIR*/smarts.

Optionally, you can specify the root of BASEDIR to be something other than C:\InCharge (on Windows), but you cannot change the *‹product›* location under the root directory.

The *EMC Smarts System Administration Guide* provides more information about the directory structure of EMC Smarts software.

EMC Smarts Service Assurance Manager

The EMC Smarts Service Assurance Manager includes the following products:

- Service Assurance Manager (Global Manager), includes Business Impact Manager (BIM) and Failover System
- Global Console
- Business Dashboard
- Companion UI
- SAM Native Adapters:
  - Service Assurance Manager Notification Adapters (E-Mail Notifier Adapter, Script Notifier Adapter, SNMP Trap Notifier Adapter, Log File Notifier Adapter)
  - Adapter Platform (Adapter Platform server, Syslog Adapter, SNMP Trap Adapter, sm_ems command-line interface)
  - XML Adapter
  - EMC Smarts Adapter for UIM/O

Related documentation

In addition to this document, EMC Corporation provides a help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs 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.

EMC Smarts documentation

Readers of this guide may find the following related documentation helpful:

- *Smarts Foundation EMC Data Access API (EDAA) Programmer Guide*
- *EMC Smarts Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products*
- *EMC Smarts Common Information Model (ICIM) Reference for Service Assurance Manager*
- *EMC Smarts Foundation Documentation Portfolio*
- *EMC Smarts System Administration Guide*
- *EMC Smarts ASL Reference Guide*
- *EMC Smarts Perl Reference Guide*
- *EMC Smarts Dynamic Modeling Tutorial*
- *EMC Smarts MODEL Reference Guide*
- *FlexNet Publisher License Administration Guide*

NOTICE

These documents are updated periodically. Electronic versions of the updated manuals are available on the EMC online support website:
https://support.emc.com

EMC Smarts Service Assurance Manager documentation

The following documents are relevant to users of the EMC Smarts Service Assurance Manager:

- *EMC Smarts Service Assurance Manager Release Notes*
- *EMC Smarts Open Source License and Copyright Information*
- *EMC Smarts Service Assurance Manager Introduction*
- *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, VoIP, and NPM Managers*
- *EMC Smarts Service Assurance Manager Deployment Guide*
- *EMC Smarts Service Assurance Manager Configuration Guide*
- *EMC Smarts Service Assurance Manager Operator Guide*
- *EMC Smarts Service Assurance Manager Dashboard Configuration Guide*

- *EMC Smarts Business Impact Manager User Guide*
- *EMC Smarts Failover System User Guide*
- *EMC Smarts Service Assurance Manager Notification Adapters User Guide*
- *EMC Smarts Service Assurance Manager Adapter Platform User Guide*
- *EMC Smarts Adapter for Unified Infrastructure Manager/Operations Configuration Guide*
- *EMC Smarts XML Adapter User Guide*
- *EMC Smarts Notification Module User Guide*
- *EMC Smarts Service Assurance Manager Troubleshooting Guide*
- *EMC Smarts Companion UI Online Help*
- *EMC Smarts Companion UI Open Source License and Copyright Information for GPLv3 as Included with a Distribution of SLES 11*
- *EMC Smarts Service Assurance Manager Documentation Portfolio*

The *EMC Smarts Documentation Catalog* provides documentation resources for other EMC Smarts products.

Conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

NOTICE is used to address practices not related to personal injury.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Pathname conventions

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

Graphical conventions

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 appears for Windows and an open circle appears for UNIX.

Manager

Unless otherwise specified, the term Manager is used to refer to EMC Smarts programs such as Domain Managers, Global Managers, and adapters.

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information. For documentation, release notes, software updates, or information about EMC products, licensing, and service, go to the EMC online support website (registration required) at:

`https://support.emc.com`

Technical support — FFor technical support, click Create Service Requests or Contact Customer Service on EMC Online Support at https://support.emc.com. To open a service request through EMC Online Support, you must have a valid support agreement. Contact your EMC Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

`techpubcomments@EMC.com`

CHAPTER 1
Architectural Overview

This chapter provides an architectural overview of EMC Smarts Service Assurance Manager (Service Assurance), the Service Assurance Manager adapters, and the Service Assurance modules (EMC Smarts Business Impact Manager, Global Console, and Business Dashboard) that can be implemented to extend the capabilities of Service Assurance.

EMC Smarts Service Assurance Manager is a solution for managing the technology infrastructure that supports business services. As the cornerstone of network operations management, it provides integrated, unified, and individualized views of the systems, network infrastructure, applications, and business entities that comprise the managed domain.

Service Assurance Manager imports topology and event information from the underlying managed domains (distributed management applications), consolidates the information, and interprets problems in the context of their impact on business services. Service Assurance provides operations personnel with meaningful information with which automated corrective actions can be associated.

The Service Assurance modules provide the capabilities to calculate the business impact of infrastructure problems, to produce a wide variety of operational and management reports, and to display customer-specific information to a given enterprise or service provider customer through a secure channel.

This chapter contains the following information:

- Service Assurance Manager architecture 14
- Service Assurance modules..... 17

Service Assurance Manager architecture

Figure 1 on page 14 illustrates the EMC® Smarts® Service Assurance Manager architecture.

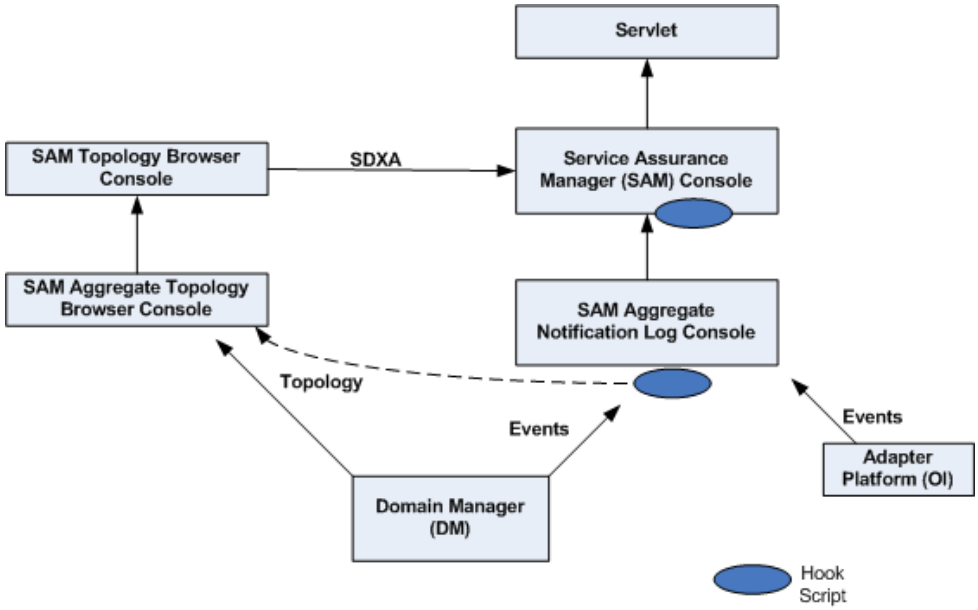

Figure 1 EMC Smarts Service Assurance Manager architecture

EMC Smarts Service Assurance Manager abstracts topology information and cross-correlates and consolidates event information from distributed EMC Smarts applications and third-party applications.

NOTICE

EMC Smarts applications are responsible for discovering and monitoring infrastructure elements, and correlating event information within their respective managed domains.

Service Assurance Manager, other EMC Smarts applications, or third-party applications communicate by way of a shared Information Bus that employs the EMC Smarts Common Information Model™ (ICIM). After Service Assurance abstracts high-level views of the distributed topologies from the underlying applications, it correlates, consolidates, and integrates event information collected from the applications, and enriches the event information with the severity of the events.

Event information (for example, root-cause problems and their impacts and severities) are displayed in the Notification Log Console, Topology Browser Console, Map Console, or Summary View Console. From these consoles, operations personnel can invoke diagnostic or corrective tools, store the information for management and operations reports, and send the information to third-party applications.

Service Assurance Manager

The Service Assurance Manager, also referred to as the Global Manager, is the Service Assurance component that serves as the central point for monitoring and managing your entire technology infrastructure by obtaining data from multiple distributed domains. The Global Manager communicates with the underlying distributed EMC Smarts applications and abstracts and consolidates:

- Network, system, application, and business resources
- Results of domain-specific root-cause analysis
- Results of domain-specific impact analysis

The Global Manager scales to large topologies because it maintains a high-level, abstract representation of the topology. The detailed topology information — and therefore the bulk of the data — is kept in other EMC Smarts applications. When needed, the Global Manager retrieves detailed information from the underlying domains.

The Global Manager can attach to multiple, distributed EMC Smarts applications as well as other Global Managers. It can also be integrated with third-party applications from which it can receive topology and event information, and to which it can send event information or initiate corrective actions.

The Global Manager, in conjunction with Report Manager, sorts and stores event-related information in an ODBC-compliant database from which users can produce a variety of management, operations, and business impact reports.

Global Console

EMC Smarts Service Assurance Manager includes a user interface that provides different views into EMC Smarts-managed domains.

The Global Console displays topology and notifications as well as summary, containment, and status information. EMC Smarts operators use the Global Console to monitor EMC Smarts domains, acquire detailed information (on demand) about topology and events, respond to problems, and take corrective action. EMC Smarts administrators with appropriate privileges and access control can use the Global Console to discover topology, and administer underlying domains, as well as administer EMC Smarts users, user profiles, program tools, and escalation policies.

The Global Console runs as a standalone Java program.

Companion User Interface

EMC Smarts Service Assurance Manager Companion User Interface (SAM Companion UI) supplements existing functionality in SAM, EMC Smarts Network Configuration Manager (NCM) and Watch4net Automated Performance Grapher (APG).

The SAM Companion UI is a VMware®-based appliance, that is, a virtual machine. The *EMC Smarts SolutionPack Installation and Configuration Guide* provides detailed information about installing and configuring the SAM Companion UI.

Integration with third-party applications

Because EMC Smarts Service Assurance Manager is an open solution, it is possible to integrate Service Assurance with third-party applications and other EMC Smarts applications by way of Service Assurance Manager (SAM) adapters, as shown in Figure 2 on page 16.

The EMC Smarts Service Assurance Manager Adapter Platform, which normalizes data in accordance with the ICIM, enables the import or export of topology and event information. The topology information is stored in the repository of the Global Manager. As event data is forwarded to Service Assurance through the adapters, the system correlates the third-party event data with the corresponding elements in the Global Manager's repository.

SAM adapters also enable EMC Smarts Service Assurance Manager to forward event information to third-party applications, such as trouble ticketing systems.

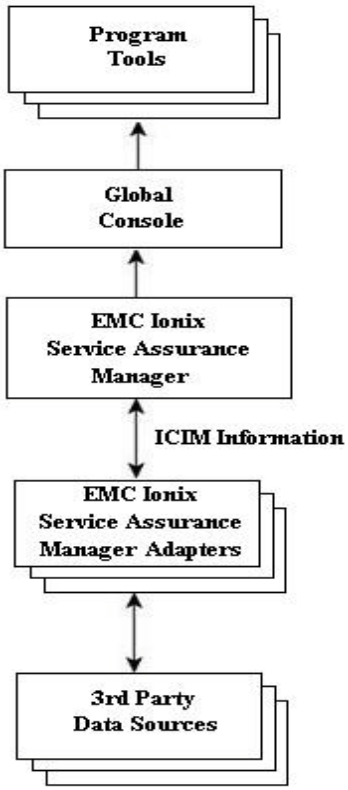

Figure 2 Integration with third-party applications

EMC Smarts Adapter for UIM/O

The EMC Smarts Adapter for Unified Infrastructure Manager/Operations (referred to as the EMC Smarts Adapter for UIM/O) provides integration between the EMC Smarts Adapter for Unified Infrastructure Manager/Operations (here in referred to as UIM/O) and the Service Assurance Manager. The adapter retrieves alerts from UIM/O, creates notifications from the alerts, and sends the notifications to the Global Manager.

The *EMC Smarts Adapter for Unified Infrastructure Manager/Operations Configuration Guide* provides deployment information, configuration instructions, and client tool examples.

Service Assurance Failover System

To maintain critical availability, EMC Smarts Service Assurance Manager can be implemented with a failover system. The EMC Smarts Service Assurance Manager Failover System ensures that the managed environment continues to be monitored when the primary Global Manager becomes unavailable because of a hardware failure or system malfunction. Redundancy is provided by a secondary Global Manager that serves as a backup to the primary Global Manager. The Failover System, which is configured to match the primary system, monitors the primary Global Manager. The Failover System periodically copies the repository file to the secondary Global Manager, thus preserving important topology and configuration information.

If a failure occurs, the secondary Global Manager automatically starts. The secondary Global Manager registers with the EMC Smarts Broker using the name of the primary Global Manager. Clients of the primary Global Manager (such as the Global Console and adapters) that become disconnected can reconnect to the secondary Global Manager.

When the primary Global Manager is again available to monitor the managed environment, a reset script copies the backup repository to the primary Global Manager, shuts down the secondary Global Manager, and restarts the primary Global Manager.

Service Assurance modules

Several modules can be implemented with EMC Smarts Service Assurance Manager to extend Service Assurance's capabilities. These include:

- EMC Smarts Business Impact Manager
- EMC Smarts Web Console
- EMC Smarts Business Dashboard

EMC Smarts Business Impact Manager

EMC Smarts Business Impact Manager (Business Impact Manager) extends the capabilities of Service Assurance to analyze events by calculating the business impact of events and propagating the impacts to affected business entities as discrete notifications that are linked to topology within the managed domain. The impacts are displayed in the Business Services Maps.

To accomplish its functions, Business Impact Manager includes facilities to import business entities, which consist of subscribers and service offerings. Subscriber information may include customers as well as organizations, business units, lines of business, and department entities. Service offerings include business processes. For example, a subscriber can be a customer that subscribes to an IT service offering that provides Internet access.

The imported business information can be also assigned to user-specified groups.

Additionally, Business Impact Manager provides facilities to assign weights to business entities and other elements in your topology. The weights capability allows you to prioritize critical topology and to use the prioritized information when calculating the business impact of events.

EMC Smarts Web Console

The contents of the Global Console can also be displayed as a Java applet within a web browser. The Web Console capability allows you to connect to a Domain Manager from any system with a web browser and does not require a Global Console installation on the system.

EMC Smarts Business Dashboard

The EMC Smarts Business Dashboard (Business Dashboard) is a flexible, business-oriented alternative to the Web Console. The Business Dashboard displays a collection of EMC Smarts analysis data alongside important data from other sources. Components of the collection of EMC Smarts data are referred to as EMC Smarts Viewlets™. The collection of viewlets can be loaded into your organization's web page and can commingle with important trouble-ticketing information or your company's intranet news. EMC Smarts viewlets can also be embedded within a third-party Web Portal product.

Figure 3 on page 18 illustrates the architecture of a Web Console and an EMC Smarts Business Dashboard when loaded by a remote user.

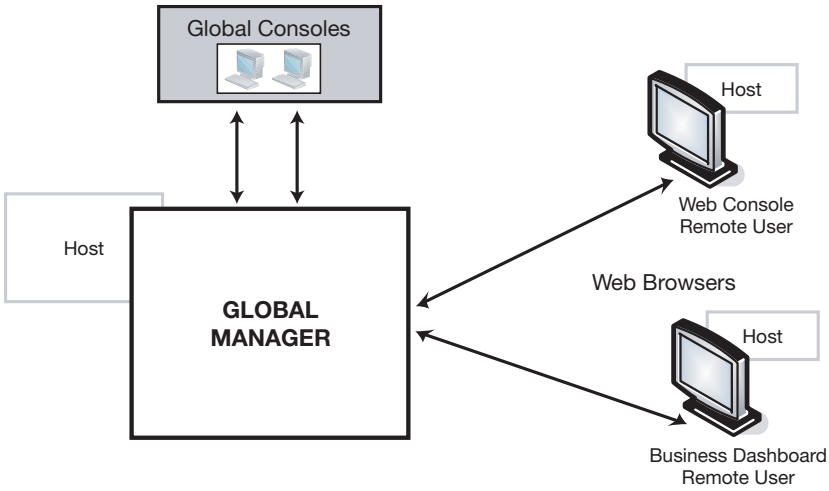

Figure 3 Web Console and EMC Smarts Business Dashboard architecture

CHAPTER 2
Functional Overview

This chapter provides a functional overview of EMC Smarts Service Assurance Manager and the Service Assurance modules (EMC Smarts Business Impact Manager, Report Manager, Web Console, and Business Dashboard) that can be implemented to extend the functionality of Service Assurance Manager. This chapter contains the following information:

- Service Assurance Manager features and functions 20
- Automatic topology and event consolidation 20
- Automatic topology abstraction 21
- Global Console 21
- Service Assurance functions 25
- Service Assurance module functions 29

Service Assurance Manager features and functions

Service Assurance Manager provides the automated functions and features that are required by today's enterprise and service provider network operations centers. Its automation, intelligent analyses, and adaptability can significantly reduce both the resources needed for pinpointing and resolving infrastructure problems, and the costs of monitoring and managing distributed networks.

Automatic topology and event consolidation

One of the primary tasks of EMC Smarts Service Assurance Manager is topology and event consolidation. Service Assurance Manager imports infrastructure elements (such as hosts and routers) and applications from each underlying managed domain. As it imports the elements, it consolidates elements that are reported by different sources. Service Assurance Manager also imports the relationships between the elements from the underlying managed domains. Using these relationships and overlapping devices, Service Assurance Manager accurately pieces together a complete topology of the managed environment.

When Service Assurance Manager imports events from the underlying managed domain, they are automatically associated with the elements to which they apply. Notifications received from multiple sources are consolidated into single events. Similarly, impacts reported by different sources for the same problem are deduplicated and associated with the consolidated event in Service Assurance Manager.

Further, to provide business context, EMC Smarts Service Assurance Manager provides a facility that imports customer and service information from provisioning systems and other sources. Using this data, Service Assurance Manager can automatically calculate the customer and service impact for the consolidated events.

Automatic topology abstraction

In order to scale to large numbers of underlying systems, EMC Smarts Service Assurance Manager performs topology abstraction. Figure 4 on page 21 illustrates the difference between a detailed representation and an abstracted representation of network connectivity.

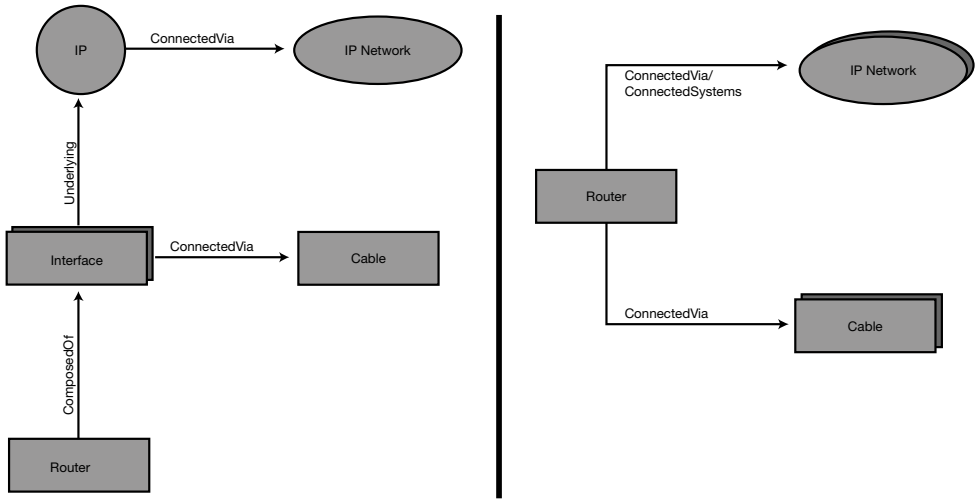

Figure 4 Difference between detailed and abstracted representation

Abstraction produces a coarse level of topology detail. A system, for example, is viewed as a single entity rather than as a collection of its components, and connectivity is between systems as opposed to between components in the system.

Although Service Assurance maintains a coarse level of topology detail, it stores sufficient information for its varied Notification Log, Topology Browser, and Map views. When needed, detailed information can be automatically retrieved from the underlying applications by Service Assurance.

Global Console

The Global Console provides a focal point through which operations personnel can monitor and manage distributed systems and EMC Smarts administrators can configure and administer Domain Managers. EMC Smarts administrators control the views, program tools, and access to console operations for EMC Smarts users. The following describes the full functionality of each console. Certain functions require a license and thus may not be included in your EMC Smarts deployment. Also, an EMC Smarts user's access to some console operations may be restricted based on the user's connection privileges and user profile.

For any given event, operations personnel with appropriate access control can take ownership of the event, acknowledge the event, add comments to the audit log of the event, or invoke tools for corrective actions.

The Global Console provides the following console views:

- Notification Log Console
- Topology Browser Console

- Map Console
- Summary View Console
- Status Table Console
- Domain Manager Administration Console
- Global Manager Administration Console

Notification Log Console

The Notification Log Console provides a view of a set of notifications, which is defined by the user profile associated with the user. The notification information can include, for example, the type of event, the element that is affected, and the severity of the event. Operations personnel can potentially open multiple Notification Log Consoles, each customized to display different events, or show multiple lists in a single console, as needed.

Operations personnel can also potentially access the details of the event through the use of the Notification Properties dialog box. The Notification Properties dialog box provides detailed information about a selected notification. The properties include, for example, attributes and values related to this event, elements that are impacted by this event, an audit log of changes in this event's history, or (if this event is a root-cause problem) other events used in the analysis.

The viewable attributes of the displayed events in the Notification Log view (for example, event severity, active event, or first notify) can be customized to meet the needs or preferences of operations personnel. The order in which the attributes are displayed can also be modified. Operations personnel can sort on any number of attributes (whether the attribute column is visible or not) by specifying up to five sorting columns.

The notifications listed in the Notification Log view are color-coded in accordance with the severity of the events. An icon is also used as another indicator of an event's severity.

Topology Browser Console

The Topology Browser Console enables operations personnel to display the managed topology in a tree format and traverse the topology. The console displays Domain Managers as well as Global Managers. For the selected managed domain, the console displays the classes of elements, instances of each class, and their relationships. Specified elements, indicated by a plus sign on Windows systems, can be expanded into instances, properties, or relationships.

When an element in the topology tree is selected, the console displays a corresponding property sheet with tabs for Attributes, Events, and Groups. The tabs, where applicable, include the following information:

- Attributes — Provides general information about the selected element
- Events — For a selected Global Manager, displays the active events that Service Assurance may notify for the element
- Groups — Provides the current group membership of the element

In addition, the Topology Browser Console provides the Browse Detail menu option. When an element in the topology tree is selected, Browse Detail displays a list of all underlying managed domains that contain that element in their topology. Users can select an underlying managed domain and display it in another Topology Browser view. For hierarchical Service Assurance deployments, users can select Browse Detail as many times as necessary to navigate to the desired domain. Note that Browse Detail is also available for selected notifications in the Notification Log Console and for selected map icons and edges in the Map Console.

Map Console

The Map Console displays, by way of icons and edges, the managed elements in a given environment and the relationships between them. Different types of maps are made available based upon the elements in your managed topology. For example, with EMC Smarts IP Availability Manager, the console displays infrastructure elements in network and connectivity maps. With the addition of Business Impact Manager, the console can also display business services maps that show how the infrastructure elements are associated with business services, as well as the customers that subscribe to those services.

Operations personnel can select elements in the maps and then display detailed information about the elements, such as the ports or interfaces contained in a system.

If the status of a given element displayed in the Map Console indicates a problem, operations personnel can view the audit logs of events by way of the Notification Properties dialog box. They can also select and use tools such as on-demand pings and Telnet sessions.

The maps can be customized to meet your needs or preferences. For example, custom backgrounds and element icons can be incorporated into the maps.

Summary View Console

The Summary View Console provides overviews or summaries of notifications. The console can contain several summaries that are attached to either the same managed domain or to different domains.

Summaries offer concise, graphical representations of sets of notifications associated with groups of elements. The summary can be depicted as a three-dimensional graph or pie chart. The summary counts indicate the percentages of elements in the group with active events.

The summaries organized by severity are color-coded in accordance with the severity of the events. Otherwise, for other criteria, the colors do not indicate event status.

Status Table Console

A Business Impact Manager user can view a Status Table to quickly determine the overall status of customers and the services being delivered to those customers. In such a Status Table, customers would be represented as the primary set of instances, and the services being delivered to them would be represented as the secondary set of instances.

To describe it in more general terms, a Status Table Console offers another way to present a concise status of a set of instances. The information appears as a matrix, with a primary set of instances along the y-axis and a secondary (related) set of instances along the x-axis. The status of the related instances appears, when relevant, at the intersection points in the matrix to reflect the overall status for each primary instance.

The Status Table functionality is very useful for the Business Impact Manager user. The Status Table requires a Web Console or EMC Smarts Business Dashboard license.

Domain Manager Administration Console

The Domain Manager Administration Console enables EMC Smarts administrators to configure and administer the underlying Domain Managers, and to perform tasks such as:

- Discover topology
- Manage and unmanage elements in the managed topology
- Access the Polling and Thresholds Console to fine-tune parameters of the polling and thresholds settings in the underlying domain

The *EMC Smarts Storage Insight for Availability Discovery Guide* provides information about the Domain Manager Administration Console. Information about polling and thresholds for specific EMC Smarts applications is provided in their respective user guides.

Global Manager Administration Console

The Global Manager Administration Console enables EMC Smarts administrators to configure Global Managers, including Security Infrastructure Managers (SIMs), and the SAM Adapter Platform.

For a selected Global Manager, EMC Smarts administrators create and maintain configuration entities such as notification lists, tools, users, user profiles, access control to console operations, and escalation policies.

The *EMC Smarts Service Assurance Manager Configuration Guide* contains information about the Global Manager Administration Console.

Service Assurance functions

The following section describes many of the functions that are integral to the EMC Smarts Service Assurance Manager.

Notification severity

The EMC Smarts Service Assurance Manager classifies notifications according to their calculated severity.

The notifications listed in the Notification Log Console and the Map Console are color-coded in accordance with the severity of the events. Icons are also used in the notification log and the maps to identify severity.

The color codes are explained in Table 1 on page 25.

Table 1 Notification severity levels

Level	Icon	Color	Description
1		Red	Critical — Identifies a specific failure that requires resolution.
2		Orange	Major — Identifies a serious condition that requires immediate attention.
3		Yellow	Minor — Identifies an abnormal condition that is not serious but requires some action.
4		Blue	Unknown — Identifies an unknown, unreachable, disconnected, or suspended condition.
5		Green	Normal — The element is in its normal state.

Notification List

A Notification List determines the events that are forwarded to a given client. Essentially, the list filters the notifications that are sent from the Global Manager to a client. Additionally, the list, which is configured by the EMC Smarts administrator, can be assigned to one or more user profiles. The personnel assigned to a specified list only see the set of events defined by the list.

The lists could be used to organize, for example:

- Business units
- Geographical regions
- Groups of resources

During day-to-day operations, operations personnel use the Global Console to monitor and manage their areas of responsibility. In doing so, personnel see only the subset of notifications defined for them in the Notification List.

EMC Smarts adapters can also connect to a Notification List, and receive the notifications that match the conditions specified in the list.

The *EMC Smarts Service Assurance Manager Configuration Guide* contains information about Notification Lists.

Tools

Tools are programs that are executed by EMC Smarts Service Assurance Manager. There are two types of tools:

- Server and client tools can be invoked by operations personnel in the Global Console or can be automated using escalation policies. Tools invoked by operators may produce output that can be sent back to the console for display.
- Automatic tools are executed by administrator-specified escalation policies or by adapters. Output is not sent back to the console for display.

Server and client tools are executed in the context of a particular target object. The target object may be a notification, or it may be an infrastructure element such as a router. When invoked from the Global Console, the specification of the target object is implicit.

Automatic tools are executed for notifications that meet the escalation criteria for specified periods of time.

The *EMC Smarts Service Assurance Manager Configuration Guide* contains additional information about the Service Assurance tools.

Notification escalation

Escalation is a process that defines a sequence of corrective actions for notifications. Examples of corrective actions include alerting responsible parties and executing automatic tools. EMC Smarts administrators use the Escalation view in the Global Manager Administration Console to configure escalation policies.

Escalation policies enable EMC Smarts administrators to automate responses to events. For example, an administrator can configure an escalation policy to page a shift supervisor if no one takes ownership of a problem for more than 15 minutes. If the problem remains unowned for 30 minutes, the policy will page the operations manager. The administrator can define multiple policies to handle different types of events.

Audit log

An audit log is associated with each of the notifications that the EMC Smarts Service Assurance Manager receives from the underlying EMC Smarts applications. The audit log includes the following information:

- Event
- Time of the update
- Name of the operations person or system that made the update
- Type of audit entry
- Description of the entry (for example, Notify, Clear, or Suspend)

Service Assurance begins to create an audit log when it receives a notification, and relates the event to an infrastructure element. Thereafter, Service Assurance adds actions for the event, any program tools used for the event, and changes in the status of the event. Actions may include system actions such as archiving and user actions such as acknowledgement and ownership. Comments can be added directly to the audit log.

An audit log for each notification can be viewed in an audit log dialog box using the Global Console, exported to spreadsheet applications, or printed as part of a report. All the audit log entries for individual notifications are stored in one log file on the Global Manager.

Containment

The Containment dialog box provides detailed information about a managed element. Containment information varies depending upon the type of element and the type of analysis being performed by the underlying domain. As examples, for a network connection, the containment information includes details about connection points; for a device managed by IP Performance Manager, containment information includes details about the device's memory.

The Containment dialog box is available for selected notifications in the Notification Log Console, for selected instances in the Topology Browser Console, and for selected nodes in the Map Console. When an element is managed by multiple Domain Managers, the Containment dialog box includes all the containment information for each domain.

Security

Security is a critical concern in the world of large-scale distributed networks. Therefore, the EMC Smarts Service Assurance Manager provides several means by which EMC Smarts administrators can set up security and control access to the system. This includes:

- User rights and privileges, including client authentication
- Encryption of passwords in files
- Encryption of communication channels
- Support for FIPS 140-2

An EMC Smarts administrator can place access restrictions on certain console operations by applying user profiles. Each user should be associated with a profile that defines the appropriate level of access control (rights and privileges) for their position and job responsibilities.

Client/server connections are controlled on both the client and server sides of the system. The system is secured using authentication records and by assigning connection privileges on the server side. When a client initiates a connection to a server, the client must supply appropriate authentication to the server before the connection (as defined by the connection privileges) is permitted.

For added protection, authentication and other passwords are encrypted in the files that store them.

Communication channels (that is, TCP connections made through Remote API) between EMC Smarts servers, brokers, and adapters can also be encrypted. Instead of passing information as clear text, these components' communications can be encrypted using

either a site secret, the Diffie Helman-Advanced Encryption Standard (DH-AES), or both. For new installations, encryption by DH-AES is enabled by default between EMC Smarts processes that support encryption.

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard governing cryptographic modules. FIPS 140 is required for any software purchased by the U.S government and U.S military. This release specifically addresses U.S Government accounts which require FIPS 140 compliance.

A configuration parameter, *SM_FIPS140*, has been introduced for FIPS 140 in the runcmd_env.sh file. The SAM administrator can enable or disable this parameter as required. The default value of this parameter is *FALSE*.

The *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, VoIP, and NPM Managers* provides additional information on FIPS 140-2.

The *EMC Smarts System Administration Guide* contains additional information about securing access to EMC Smarts applications. The *EMC Smarts Service Assurance Manager Configuration Guide* includes additional information about restricting access to certain Global Console operations.

Service Assurance module functions

The Service Assurance modules provide additional capabilities to calculate the business impact of infrastructure problems, to produce a wide variety of operational and management reports, and to display customer-specific information to a given enterprise or service-provider customer through EMC Smarts Business Dashboard.

EMC Smarts Business Impact Manager functions

The degradation or failure of important infrastructure elements can slow or stop vital business processes and business services, or dramatically reduce user productivity in needed business areas. EMC Smarts Business Impact Manager ensures maximum availability of services.

EMC Smarts Business Impact Manager (Business Impact Manager) extends the capabilities of Service Assurance to calculate the business impact of events, and to propagate the impacts to affected business entities as discrete notifications that are linked to elements in the infrastructure.

Users can create business entities, such as organizations, business units, lines of business, and departments, and relate them to corresponding infrastructure elements. Users can also create business processes.

In Business Impact Manager, users can assign different weights to any elements in the business or infrastructure topology. Business Impact Manager calculates the impact of root-cause problems by summing up the weights of the impacted elements.

The calculated impact enables operations management to prioritize notifications in accordance with business needs, and to effectively use their time and resources to resolve problems that degrade or threaten vital processes and services.

Business process tools are also provided for users to create, update, and delete events associated with their business processes. For example, a user might create an event that represents a telephone call from a supplier who is out of stock of a popular retail product, and then associate the event with the user's Order Fulfillment Business Process.

The *EMC Smarts Business Impact Manager User Guide* includes detailed information regarding Business Impact Manager.

EMC Smarts Business Dashboard functions

The EMC Smarts Business Dashboard (Business Dashboard) displays views normally available from the Global Console as a collection of EMC Smarts viewlets within your organization's web page or a third-party web portal. EMC Smarts viewlets can display a variety of information including a Notification Log, Status Table, Map, Summary, Notification Properties, or Containment view. Viewlets can also be customized to suit your needs. For example, a map viewlet can be set up to show a specific topology instance as the focus of the map display.

Furthermore, the viewlets can function as sources for broadcasting context information to other, listener viewlets. For example, a Status Table viewlet and a Notification Log viewlet can be displayed such that selections in the Status Table result in the Notification Log showing notifications related to those Status Table selections.

CHAPTER 3
Implementation Scenarios

This chapter highlights important features of EMC Smarts solutions, and describes how EMC Smarts Service Assurance Manager can be implemented for a competitive advantage in two business areas:

- Enterprise service provider
- Network service provider

This chapter contains the following information:

- Challenges of network management 32
- EMC Smarts solutions 32
- Enterprise provider 34
- Network service provider 36

Challenges of network management

Regardless of the business area, network management organizations everywhere are faced with the following challenges:

- Improve service
- Reduce operational costs
- Integrate new tools with existing management and support systems
- Deliver a high return on investment

EMC Smarts solutions

The features and functions of the EMC Smarts solutions, which include EMC Smarts IP Availability Manager, EMC Smarts IP Performance Manager, EMC Smarts Application Services Manager, EMC Smarts ATM/Frame Relay Manager, and EMC Smarts Service Assurance Manager, address important challenges that network management organizations face on a day-to-day basis.

Fast and accurate fault isolation

EMC Smarts uses comprehensive topology models to quickly and accurately analyze and isolate failures in networks of any size and complexity.

EMC Smarts analysis improves service by greatly reducing manual problem isolation, which accounts for up to 80 percent of total downtime. The analysis also lowers operational costs by reducing the human effort involved in isolating problems, as well as the effort involved in chasing down all the symptomatic events and false alerts.

Automated corrective actions

Once a fault has been accurately isolated, Service Assurance Manager can be configured to initiate automated responses to correct soft faults or to reroute services around failures. Because EMC Smarts can separate root-cause problems from symptomatic events and false alarms, actions are only invoked when or where needed. With the EMC Smarts topology models, corrective actions can be invoked against both the failed component or any impacted services.

Service Assurance Manager's automated actions avoid service downtime and provide virtually immediate service restoration. They can also improve service by fixing problems before users become impacted.

Business focus

EMC Smarts Business Impact Manager can import business information directly from existing data sources such as provisioning systems. During its analysis, it places infrastructure problems in their proper business context and analyzes their impact on services, business processes, and customers. This enables managers to focus their efforts on the problems with the highest business impact.

Integration

EMC Smarts solutions are designed to integrate with management tools and other operational support systems. EMC Smarts leverages management data from third-party sources while providing console access to third-party management applications. EMC Smarts software's ability to distill countless events into a concise set of defined problems and exceptions makes it a natural integration point for problem management (ticketing) systems.

Service Assurance's integration with other management applications lowers operational costs by providing users with a single, consistent, intuitive interface for viewing all management data. At the same time, Service Assurance improves operational control by presenting a concise display of network problems in their full topology context, complete with their impacts and histories.

Rapid deployment and low maintenance

EMC Smarts solutions are designed for rapid deployment and low maintenance. Unlike other management solutions, EMC Smarts software's comprehensive set of problem and impact models automatically adapt to the configuration of the network infrastructure — providing immediate results. This same adaptability enables EMC Smarts solutions to automatically keep pace with future changes in the infrastructure without the need for expensive ongoing code maintenance.

EMC Smarts has the ability to automatically adapt to changes due to use of ICIM models that represent the various elements of the infrastructure, how they relate to one another, and how they can affect one another. EMC Smarts solutions then apply these models to the discovered elements in a given network to provide problem and impact analysis specific to that network. Furthermore, customers who need additional functionality can leverage these models to build solutions that also adapt automatically to change.

This enables EMC Smarts solutions to provide better return on investment than other management solutions. Benefits include:

- Automatic adaptation reduces the head-count needed to maintain the management solution
- Analysis that automatically adapts to changes in the environment and provides more accurate results, which reduces service downtime
- More accurate analysis frees up expensive engineering resources to work on more strategic initiatives

Enterprise provider

A diversified financial services firm deployed an EMC Smarts Service Assurance Manager solution to help them manage their complex infrastructure as an integrated system rather than as sets of unrelated silos.

The primary concern of the financial enterprise was that more than 100 mission-critical applications were used by their business units, such as applications to monitor their exposure to interest and currency fluctuations. Basically, the enterprise had too many mission-critical applications for the network teams to track. At the same time, their network changed and evolved so quickly that the application teams could not stay abreast of the changes.

As a result, when network failures occurred, or when network maintenance was required, they had no way of knowing which applications were affected. Attempts to do this with traditional tools—where one specified network dependencies for each application—failed because of the need to manually maintain the correlation logic every time the network topology changed. If they missed a change, the correlation would fail.

By deploying an EMC Smarts solution, the enterprise was able to solve their problem by separating the network, applications, and business analysis into separate domains, thus breaking the problem into manageable pieces, as well as automating the most complicated part of their problem: defining the network dependencies of the distributed applications. Their EMC Smarts solution consisted of the following:

- EMC Smarts IP Availability Manager and IP Performance Manager — To monitor failures in the network infrastructure and identify the affected systems, automatically calculating the affect of any network path redundancies
- EMC Smarts Application Services Manager — To perform root-cause and impact analysis of distributed applications based on events and topology information imported from the IP Availability Manager, IP Performance Manager, and the SAM adapters
- EMC Smarts Business Impact Manager — To correlate failures in the technology infrastructure to the businesses they impact (for example, processing on NASDAQ trades)
- EMC Smarts Service Assurance Manager — To bring it together into a single system, where users can customize views of the data they need, and use the appropriate tools to quickly restore service
- EMC Smarts Business Dashboard — To provide web-based, personalized views for business unit managers (for example, in the foreign exchange unit) showing a map representation and a summary view of the status of their systems.

Figure 5 on page 35 illustrates their EMC Smarts implementation.

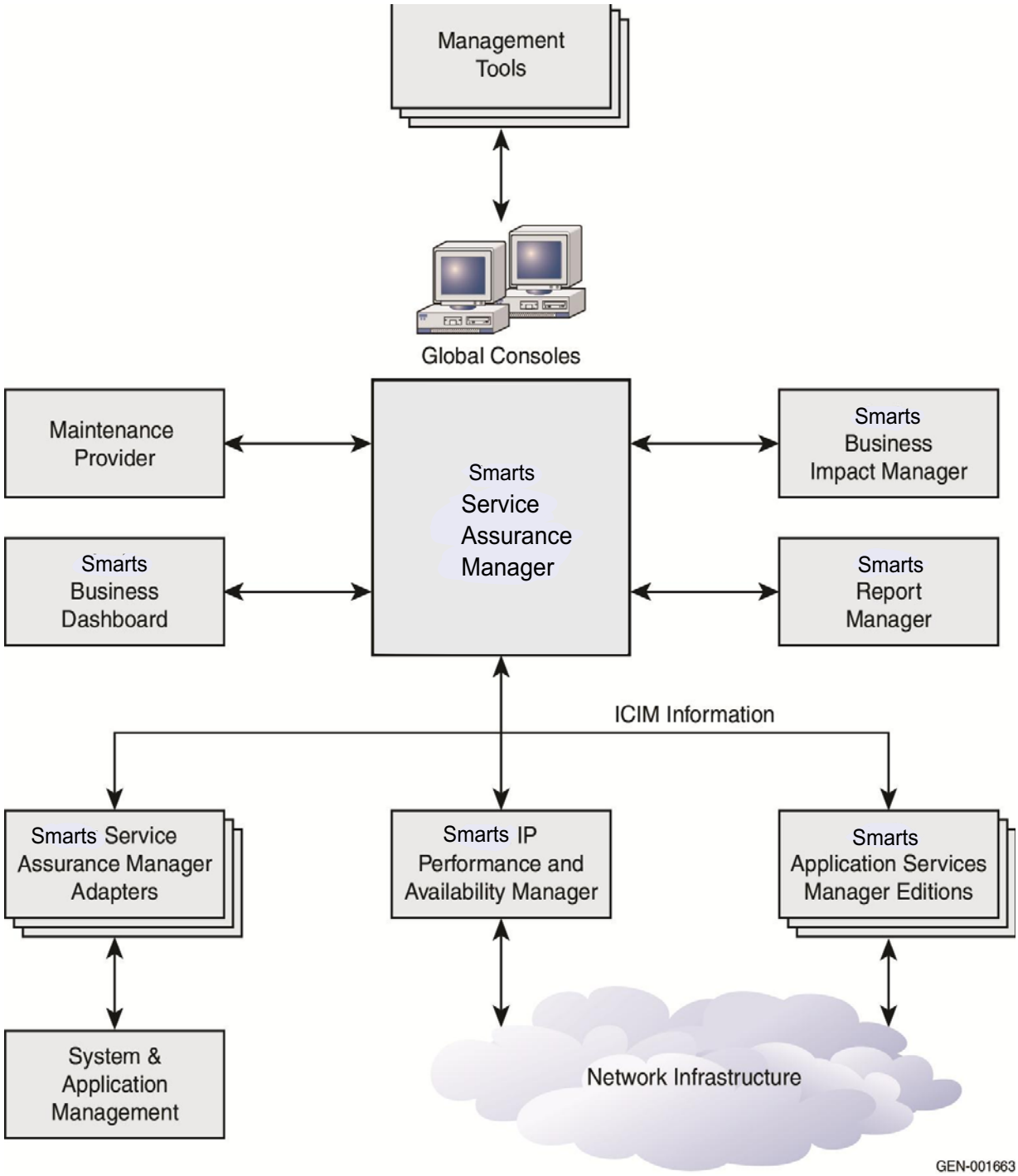

Figure 5 Enterprise solution

By connecting the analysis from the network, application, and business domains, EMC Smarts Service Assurance Manager provided the enterprise with an end-to-end view of causes and impacts — automatically correlating network failures with their impacts on applications and critical business processes.

By knowing the business impact of each problem, the operations staff effectively prioritized their support efforts on the most critical problems; that is, they aligned their efforts with the overall business objectives of the enterprise.

At the same time, because EMC Smarts IP Availability Manager and EMC Smarts IP Performance Manager automatically adapt to changes in the network topology, operations did not need to devote teams of people to modify the analysis every time the network topology changes. This dramatically reduced the cost to maintain their management systems. In fact, because all of the logic is based on the infrastructure topology, they only needed to manually maintain the business and application elements. EMC Smarts software automatically adapted everything else: root-cause and impact analysis, personalized views, and so forth.

In addition to solving the problem of application and business impact, the EMC Smarts Service Assurance Manager also streamlined operational processes.

By identifying the root causes, the support staff eliminated most of the time-consuming fault isolation process and immediately proceeded to problem resolution. By identifying which events are impacts of other problems, the support staff avoided wasting time trying to chase down and fix symptoms of other problems. Finally, by relating the root causes with the impacts, operations staff streamlined communications. For example, when estimating the time to resolve a root-cause problem, that information was automatically propagated to all affected systems, applications, and business processes.

Because they identified the actual root-cause failures (for example, a card on a switch), they were able to automate the dispatch of service technicians from their maintenance provider. More importantly, because they positively identified the failed element, they avoided the delays caused by technicians who arrived on site with the wrong parts.

By integrating the EMC Smarts solution with their existing system and application management tools (by way of SAM adapters), the enterprise was able to leverage their previous investments in management tools and accelerate the deployment of the overall solution.

Network service provider

A large network service provider had been using traditional management tools to manage a broad array of services. After several years of deployment and custom work, the systems were starting to improve network operations. However, the maintenance costs were spiraling out of control and it was becoming more difficult to keep up with changes in the managed environment. Worse, the operational improvements were not translating into higher customer satisfaction because of communications failures between operations and the call center. The provider needed to find an alternative that could deliver real improvements to customer satisfaction while reducing operational costs. The answer to this challenge was an EMC Smarts solution composed of:

- EMC Smarts ATM/Frame Relay Manager
- EMC Smarts IP Availability Manager

- EMC Smarts IP Performance Manager
- EMC Smarts Application Services Manager
- EMC Smarts Service Assurance Manager Adapter Platform
- EMC Smarts Business Impact Manager
- EMC Smarts Service Assurance Manager
- EMC Smarts Business Dashboard

With the autodiscovery feature of EMC Smarts autodiscovery, built-in analysis, and policy-based management, operations was able to immediately identify and isolate root-cause failures in their networks. Because EMC Smarts applications automatically detect and adapt to changes in topology, the service provider no longer needed to dedicate teams of consultants to maintain them. Also, because EMC Smarts intelligently manages networks with overlapping IP addresses (for example, private IPs), the provider could discontinue the expensive process of dedicating a separate management system to each customer. These features helped the provider to dramatically reduce the cost of managing their environment.

By integrating the EMC Smarts solution with existing management tools (for example, system and application agents from Concord), the service provider was able to use its existing investments to cut deployment time.

The unique capability of EMC Smarts to integrate not just events, but events in the context of a comprehensive topology, allowed the service provider to more effectively integrate operations with its other OSS applications. By integrating with their provisioning system, the provider was able to automatically build their business topology, and relate customers to services and services to elements in their network topology. This integration provided automated business impact analysis for prioritization, and allowed users to view technology failures in their complete technical *and* business context.

Leveraging this business topology, EMC Smarts was able to automatically identify which events customers would care about so that the call center could focus on customer impacts rather than sifting through masses of arcane infrastructure events. Similarly, by using the customer data to integrate with the CRM application, EMC Smarts was able to identify the account managers associated with each customer impact, and notify them of problems in real time. Furthermore, the operations staff used this information to coordinate maintenance work with the account managers of potentially affected customers.

Because problem causes and impacts were linked, the provider was also able to streamline communications between operations and the call center. For example, when operations identified a problem and dispatched an engineer to resolve it, they could estimate a repair time and the system automatically relayed that estimate for all customer impacts to the call center and customer web applications so that everyone immediately knew when the service would be restored. Finally, when customer relations faced a crisis and the customer assurance staff elevated the priorities of specific customer impacts, EMC Smarts automatically applied the priority changes to the root-cause failures and notified engineering management so that operations could shift their activities accordingly.

With the Business Dashboard, the provider's customers were able to get real-time views of their data. Because these views use the same topology, the views changed automatically whenever the topology changed. This, too, reduced the cost of servicing customers.

In conclusion, by effectively integrating the EMC Smarts solution with its existing applications (for example, provisioning, CRM, and call center), the service provider was able to show a more professional face to its customer. In the past, customer calls to the call center typically resulted in an operator taking messages, calling around operations to see what was happening, and then calling the customer back — a time- consuming process that often left the customer wondering what the provider was doing. Now, when the customer calls, the call center is not only aware of the problem, but is also able to give the customer up-to-the-minute information about the status of the problem and its resolution.

INDEX

A
adapter 27, 36, 38
    and third-party applications 18
    SAM Adapter Platform 26
architecture
    Service Assurance Manager 16
audit log 23, 24, 28
audit logs 25

B
Business Dashboard 20, 31, 36
    architecture 20
    sources for listener viewlets 31
Business Dashboard functions 31
business focus 34
Business Impact Manager 19, 31, 36
    functions 31
business services maps 25

C
challenges of network management 34
Containment dialog box 29
corrective actions 34

D
Diffie Helman-Advanced Encryption Standard 30

E
EMC online support website 9
EMC Smarts Application Services Manager 34, 36
EMC Smarts ATM/Frame Relay Manager 34
EMC Smarts IP Availability Manager 25, 34, 36
EMC Smarts IP Performance Manager 34, 36
EMC Smarts Service Assurance Manager 22, 34, 36, 38
EMC Smarts solutions 34
    enterprise service provider 37
encryption 30
enterprise service provider 33, 36
escalation 28
event consolidation 22

F
fault isolation 34
features and functions, Service Assurance Manager 22
functional overview 21
functions, Service Assurance modules 31

G
Global Console 17, 20, 23
    Domain Manager Administration Console 26
    Map Console 25
    Notification Log Console 24
    Status Table Console 25
    Summary View Console 25
    Topology Browser Console 24
Global Manager 17, 18, 19, 27, 29

I
implementation scenarios 33
Information Bus 16
integration 18, 35

N
network service provider 38
notification
    escalation 28
    properties 24
    severity 27
Notification List 27
Notification Properties dialog box 24

P
property sheet 24

R
rapid deployment 35
Report Manager 19
reports 15, 16, 29, 31

S
security
    accessing 29
    Diffie Helman-Advanced Encryption Standard 30
Service Assurance Failover System 19
Service Assurance Manager 22, 34, 36, 38
Service Assurance modules 15, 19, 21
    Business Dashboard 19, 20
    Business Impact Manager 19
    Report Manager 19
    Web Console 19, 20
service provider 39
severity color codes 27
Status Table Console 25
    licensing 26

T
tools 28
topology
    abstraction 23
    event consolidation 22

W

Web Console 19, 20