Preface ................................................................................................................................................... vii

Chapter 1 Overview of the Service Assurance Deployment Process

EMC Smarts architecture .................................................................................................................. 1-2
The deployment process .................................................................................................................. 1-4
  Stage 1: Designing the deployment ............................................................................................. 1-4
  Stage 2: Installing and configuring the components ............................................................... 1-5
  Stage 3: Validating the deployment ........................................................................................... 1-6
  Stage 4: Monitoring and tuning the deployment ....................................................................... 1-6
Before you begin checklist ............................................................................................................ 1-7

Chapter 2 Gathering Basic Information

Document the deployment .............................................................................................................. 2-2
  The Solution Architecture Diagram ....................................................................................... 2-2
  The Deployment Build Guide ............................................................................................... 2-2
Determine the organization’s requirements .................................................................................. 2-3
  Obtain network and application information ......................................................................... 2-3
  Determine network and application priorities ......................................................................... 2-5
Gather information required to size Service Assurance ............................................................... 2-6
  Determine how many devices and applications will be managed ........................................ 2-6
  Estimate quantities and types of Service Assurance clients ................................................ 2-6
  Estimate the number of underlying EMC Smarts domains .................................................... 2-7
Determine requirements for installing software ........................................................................... 2-8
  Define requirements for integrating existing software with EMC Smarts ........................... 2-8
Gather network security information ............................................................................................ 2-9
  Firewalls between parts of the EMC Smarts deployment ......................................................... 2-9
What other network features affect EMC Smarts? ...................................................................... 2-10
Basic Service Assurance information checklist ........................................................................ 2-11

Chapter 3 Designing the Service Assurance Deployment

Determine the Service Assurance configuration ......................................................................... 3-2
  Standard Global Manager configuration ............................................................................... 3-3
  Basic hierarchical Global Manager configuration ............................................................... 3-3
  Hierarchical aggregation Global Manager configuration .................................................... 3-4
  Hierarchical presentation Global Manager configuration .................................................... 3-5
  Hierarchical Mesh Global Manager configuration ............................................................... 3-6
Hardware for Service Assurance platform equipment tiers ....................................................... 3-7
Contents

Deploying Global Managers and Domain Managers ........................................ 3-8
Adding information to the Solution Architecture Diagram and Build Guide .......... 3-8
Essential EMC Smarts applications ................................................................... 3-9
Locating EMC Smarts Brokers ........................................................................ 3-9
Locating license servers .................................................................................. 3-9
Locating the Global Managers in the network .................................................. 3-11
Considering security and firewalls ................................................................. 3-12
Considering failover (high availability) configurations ....................................... 3-13
Designing acceptance tests ............................................................................. 3-14
Initial design checklist ..................................................................................... 3-15

Chapter 4 Designing for Topology Operations
Designing topology synchronization ................................................................. 4-2
Understanding topology synchronization ......................................................... 4-2
Planning for topology synchronization ............................................................. 4-3
Designing topology groupings ......................................................................... 4-4
Designing topology operations checklist .......................................................... 4-5

Chapter 5 Planning for Notifications
Overview of notification processing .................................................................... 5-2
Notifications from the Adapter Platform ............................................................ 5-3
Configuring notifications for clients .................................................................. 5-3
Designing trap processing ................................................................................. 5-4
Recommended trap processing design ............................................................... 5-4
Trap forwarding ................................................................................................. 5-6
Trap processing performance ............................................................................ 5-7
Filtering traps in trap_mgr.conf ....................................................................... 5-7
Using trap manager hook scripts ..................................................................... 5-7
Adding new topology for received traps ............................................................ 5-7
Looking up host names ...................................................................................... 5-7
Batching traps .................................................................................................... 5-7
Planning for notifications checklist ................................................................. 5-9

Chapter 6 Designing for EMC Smarts Users
Who are the Global Manager users? .................................................................. 6-2
Choose a console for types of users .................................................................... 6-3
Deployment considerations for client consoles .................................................. 6-3
Users and security .............................................................................................. 6-4
Designing user profiles ...................................................................................... 6-5
Designing notification lists ............................................................................... 6-5
Restricting console operations ......................................................................... 6-5
Designing consoles ............................................................................................ 6-5
Planning for tools and tool deployment ............................................................. 6-6
EMC Smarts user design checklist ..................................................................... 6-7

Chapter 7 Deploying Business Impact Processing
Designing business impact processing ............................................................... 7-2
Business processes ............................................................................................ 7-2
Business topology .............................................................................................. 7-2
Weights: Impacts of issues in the topology .......................................................... 7-3
Importing information ....................................................................................... 7-4
The structure of import files ................................................................. 7-4
Integrating with EMC Smarts Application Insight................................... 7-4
Business Impact Manager design checklist........................................... 7-5

Chapter 8  Deploying Service Assurance

General installation/deployment guidelines .............................................. 8-2
EMC Smarts licensing ............................................................................. 8-2
EMC Smarts Service Assurance installation and configuration .............. 8-3
Configure security .................................................................................. 8-3
Deploy Business Impact Manager......................................................... 8-4
Deploy user configurations................................................................. 8-4
Configuring the Java clients to use a proxy server .................................. 8-5

Chapter 9  Validating Your Deployment (Acceptance Testing)

Validation techniques ........................................................................... 9-2
Initial validation ..................................................................................... 9-2
Validating topology operations.............................................................. 9-2
Validating users and capabilities ......................................................... 9-2

Chapter 10 Monitoring the Performance of Your Deployment

Assessing performance ......................................................................... 10-2
Monitor Global Manager memory usage ............................................... 10-2
Monitoring Global Manager queues ..................................................... 10-3
Monitoring with heartbeat notifications ............................................... 10-5
Monitoring topology synchronization .................................................. 10-6
Periodic dump threads and dump clients ............................................. 10-7
Monitoring tools .................................................................................. 10-9
Monitoring escalation ......................................................................... 10-9
Improving performance ........................................................................ 10-11
Refine notification lists for users ......................................................... 10-11
Reassess configuration of topology synchronization ......................... 10-11
Refine set of trap and syslog notifications sent to Global Manager .... 10-11
Increase worker threads for escalation ............................................... 10-12
Upgrade server hardware ................................................................... 10-12
Redesign the Service Assurance deployment ..................................... 10-12

Appendix A  Design and Deployment Checklists

Before you begin checklist ..................................................................... A-2
Basic information checklist .................................................................. A-3
EMC Smarts design checklist ................................................................ A-4
Designing topology operations checklist ............................................. A-5
Planning for notifications checklist ..................................................... A-6
EMC Smarts client and user design checklist ...................................... A-7
Business Impact Manager design checklist ....................................... A-8

Index .................................................................................................. i-1
The **EMC Smarts Service Assurance Management Suite Deployment Guide** describes how to deploy the EMC Smarts Service Assurance Management Suite and related components of the EMC Smarts Service Assurance Management Suite.

This guide is intended as a comprehensive resource for deployment tasks. In many cases, you will be referred to other EMC Smarts documents for specific procedures and configuration tasks, such as:

- Consult the **EMC Smarts Service Assurance Management Suite Installation Guide** that accompanied your software product suite for detailed hardware requirements, platform requirements, and installation procedures.
- Consult the **EMC Smarts Service Assurance Manager Configuration Guide** for information about the Global Manager Administration Console.
- Consult the **EMC Smarts System Administration Guide** for detailed administration procedures for the EMC Smarts deployment.

**Audience for this guide**

This guide is intended for the following audiences:

- Network and system administrators who aid in designing and maintaining EMC Smarts deployments
- Integrators and network consultants who aid in designing EMC Smarts deployments and then install, validate, and tune the deployments
- Systems engineers who design EMC Smarts deployments
- EMC Smarts Professional Services personnel who design, install, validate, and tune EMC Smarts deployments
- EMC Global Services personnel who respond to inquiries, problems, and issues that arise during EMC Smarts deployments

**EMC Smarts Service Assurance Management Suite installation directory**

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

For UNIX, this location is: `/opt/InCharge<n>/<productsuite>`.

For Windows, this location is: `C:\InCharge<n>\<productsuite>`.

The `<n>` represents the software platform version number. The `<productsuite>` represents the EMC Smarts product suite to which the product belongs. For example,
on UNIX operating systems, EMC Smarts Service Assurance Management Suite is, by
default, installed to /opt/InCharge7/SAM/smarts. On Windows operating systems,
this product is, by default, installed to: C:\InCharge7\SAM\smarts. This location is
referred to as BASEDIR/smarts.

Optionally, you can specify the root of BASEDIR to be something other than
/opt/InCharge7 (on UNIX) or C:\InCharge7 (on Windows), but you cannot change
the <productsuite> location under the root directory.

For more information about the directory structure of EMC Smarts software, refer to
the EMC Smarts System Administration Guide.

EMC Smarts Service Assurance Management Suite

The EMC Smarts Service Assurance Management Suite includes the following
products:

- Service Assurance Manager (Global Manager), includes Business Impact
  Manager (BIM) and Failover System
- Global Console
- Business Dashboard
- 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

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

EMC Smarts documentation

Readers of this guide may find the following related documentation helpful. It can be
found in the BASEDIR/smarts/doc/pdf directory.

Note: These documents are updated periodically. Electronic versions of the updated manuals
are available on the Powerlink website:

- EMC Smarts Documentation Catalog
- EMC Smarts System Administration Guide
- EMC Smarts ICIM Reference
- EMC Smarts Common Information Model Infrastructure Models Chart
- EMC Smarts Common Information Model Application-Business Models Chart
- EMC Smarts ASL Reference Guide
EMC Smarts Service Assurance Management Suite documentation

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

- **EMC Smarts Service Assurance Manager Introduction**
- **EMC Smarts Service Assurance Management Suite Deployment Guide**
- **EMC Smarts Service Assurance Management Suite Installation Guide**
- **EMC Smarts Service Assurance Manager Operator’s Guide**
- **EMC Smarts Service Assurance Manager Configuration Guide**
- **EMC Smarts Service Assurance Manager Dashboard Configuration Guide**
- **EMC Smarts Business Impact Manager User’s Guide**
- **EMC Smarts Report Manager User’s Guide**
- **EMC Smarts Service Assurance Manager Failover System User’s Guide**

Refer to the **EMC Smarts Documentation Catalog** for documentation resources provided with other EMC Smarts product suites.

Suggestions for searching PDF files

You may search across multiple PDF files using the Adobe Acrobat Reader software.

1. If the documentation is not accessible to all users of the EMC Smarts product suite, copy the contents of the `/BASEDIR/smarts/doc/pdf` directory to a central location, such as a shared drive on your LAN, that operators and others may view.

2. To search throughout the documentation library, open the Acrobat Reader software.
   1. Choose **Edit > Search**, and enter a word or phrase.
   2. In the **Where would you like to search** option, select **All PDF Documents in** and type the pathname of the location where the PDF documents reside.

If you have more than one EMC Smarts product suite installed, you can set up cross-product document searches by copying files from the `/BASEDIR/smarts/doc/pdf` directory for each product suite into this common documentation directory path.

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

**Note**: A note presents information that is important, but not hazard-related.

**IMPORTANT**

An important notice contains information essential to the operation of the software.
CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

Typographical conventions

EMC uses the following type style conventions in this guide:

**Normal font**

In running text:
- Interface elements (for example, button names, dialog box names) outside of procedures
- Items that user selects outside of procedures
- Java classes and interface names
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities
- Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications

**Bold**

In procedures:
- Names of dialog boxes, buttons, icons, menus, fields
- Selections from the user interface, including menu items and field entries
- Key names
- Window names

In running text:
- Command names, daemons, options, programs, processes, notifications, system calls, man pages, services, applications, utilities, kernels

**Italic**

Used for:
- Full publications titles referenced in text
- Unique word usage in text

**Courier**

Used for:
- System output
- Filenames
- Complete paths
- command-line entries
- URLs

**Courier, bold**

Used for:
- User entry
- Options in command-line syntax

**Courier, italic**

Used for:
- Arguments used in examples of command-line syntax
- Variables in examples of screen or file output
- Variables in path names

< >

Angle brackets used to enclose parameter or variable values supplied by the user.

[ ]

Square brackets used to indicate optional values.

| |

Vertical bar used to indicate alternate selections. The bar means “or”.

{ }

Braces used to indicate content that you must specify (that is, x or y or z).

...

Ellipses used to indicate nonessential information omitted from the example.

%  

Used to indicate a C shell prompt.

#  

Used to indicate a C shell superuser prompt.

▼▲  

Used to indicate a command is wrapped over one or more lines. The command must be typed as one line.
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 displays for Windows and an open circle displays for UNIX.

Smarts Manager
Unless otherwise specified, the term Smarts 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 for information about EMC products, licensing, and service, go to the EMC Powerlink™ website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Sales and customer service contacts — For the list of EMC sales locations, please access the EMC home page at:

http://EMC.com/contact
This chapter provides an overview of the deployment process for the Service Assurance portions of the EMC® Smarts® architecture and contains the following information:

- EMC Smarts architecture ................................................................. 1-2
- The deployment process ................................................................. 1-4
- Before you begin checklist ............................................................. 1-7
EMC Smarts architecture

The EMC Smarts Service Assurance Management Suite is a fundamental part of all EMC Smarts deployments. As shown in Figure 1-1 on page 1-3, the suite consists of the following components and relationships:

- The Global Manager (Service Assurance Manager) is a manager of managers (MoM) that provides end-to-end views of the status of your managed IT environment. The Global Manager consolidates and abstracts topology, analysis, and events from various sources, including EMC Smarts Domain Managers such as EMC Smarts IP Availability Manager and EMC Smarts IP Performance Manager. In addition, the Global Manager serves as an integration point for the EMC Smarts product suites.

- The EMC Smarts Business Impact Manager allows you to create and relate business-level objects, such as departments, services, and customers, to applications and network infrastructure. The Business Impact Manager can then determine the business impact of infrastructure failures on business services and their users. The Business Impact Manager is installed as part of the Global Manager.

- The EMC Smarts Global Console is a user interface that provides information about EMC Smarts analysis: root-cause failures, notifications, topology, and even business views. The Global Console also provides configuration and administration controls. This functionality can also be provided to a web browser using a Java applet as the EMC Smarts Web Console. Both the Web Console and Global Console connect directly to the Global Manager.

- The Business Dashboard is a flexible, business-oriented alternative to the Web Console. With the Business Dashboard, a collection of EMC Smarts analysis data can be displayed with important data from other sources on an organization’s web page. Each component of EMC Smarts data is referred to as a Dashboard viewlet, which connects directly to the Global Manager.

- EMC Smarts Service Assurance Adapters (SAM Adapters) and the EMC Smarts Service Assurance Manager Adapter Platform (Adapter Platform) provide EMC Smarts software with additional sources of data when monitoring a network. The Adapter Platform normalizes and consolidates data from adapters before it is passed to Service Assurance. This guide covers deployment of the Adapter Platform and specifically describes two adapters that send data to the Adapter Platform: the EMC Smarts SNMP Trap Adapter and the EMC Smarts Syslog Adapter.

Product suites such as the EMC Smarts IP Management Suite, EMC Smarts Application Services Management Suite, and the Network Protocol Management Suite include Domain Managers that discover and/or monitor objects for a particular domain.

The Domain Managers use Codebook Correlation Technology™ to perform root-cause analysis for the related domain. These domains forward topology and events to the Global Manager, which provides this information, consolidated and abstracted, to the Global Console.

Design and deployment of the underlying Domain Managers is not covered in this guide. Deployment of the EMC Smarts IP Management Suite is described in the EMC Smarts IP Management Suite Deployment Guide.
Figure 1-1 EMC Smarts Service Assurance Management Suite deployment architecture
The deployment process

EMC Smarts software is deployed in phases. In the first phase, the domains that feed the EMC Smarts Service Assurance Management Suite are deployed. If there are many types of underlying EMC Smarts domain, each type can be deployed in a separate phase. The sequence of these initial phases is determined by the priorities of the organization and the complexity of each domain.

An EMC Smarts Service Assurance Management Suite is typically deployed in the initial phases with these underlying EMC Smarts domains, but only in a simple, standard configuration. This deployment is intended only to validate the operation of the EMC Smarts domains and is described in the deployment guide for that domain.

After the initial phases, the production design of the EMC Smarts Service Assurance Management Suite configuration is deployed. This deployment phase is covered in this guide and includes the design, installation, and configuration of EMC Smarts Service Assurance Management Suite. Specific installation and configuration details are described in the *EMC Smarts Service Assurance Management Suite Installation Guide* and the *EMC Smarts Service Assurance Manager Configuration Guide*.

As shown in Figure 1-2, each phase in the deployment process can be further divided into four distinct stages:
- Stage 1: Designing the deployment
- Stage 2: Installing and configuring the components
- Stage 3: Validating the deployment
- Stage 4: Tuning and maintaining the deployment to improve performance

During each stage of deployment, it is vitally important that you document all aspects of the deployment that could be required to recreate, troubleshoot, and reconfigure the installation. Creating a document for this information is described in “Document the deployment” on page 2-2.

Stage 1: Designing the deployment

Designing an EMC Smarts deployment consists of gathering necessary information and then using the information to develop a plan for the deployment.

Gathering the information is a process that involves both the designer and the network and application administrators. The administrators must provide details of
their organization’s network and application infrastructure. This process is described in “Gathering Basic Information” on page 2-1.

This information is then applied to develop a deployment design that will properly support the infrastructure. The design should also account for projected growth of the network and applications.

While the deployment is being designed, all plans, decisions, and supporting information must be documented. Typically, this documentation takes the form of a Solution Architecture Diagram and a Deployment Build Guide. In their preliminary stages, this diagram and guide may be used in the response to an organization’s Request for Proposal (RFP) or Request for Quote (RFQ).

Once a deployment is contracted, the information in the Solution Architecture Diagram and Deployment Build Guide can be refined and verified.

Design is covered in the following chapters:

◆ “Designing the Service Assurance Deployment” on page 3-1
◆ “Designing for Topology Operations” on page 4-1
◆ “Planning for Notifications” on page 5-1
◆ “Designing for EMC Smarts Users” on page 6-1
◆ “Deploying Business Impact Processing” on page 7-1 (optional)

Normally, this design process is performed by EMC Smarts Professional Services or an EMC Smarts partner with extensive input from the organization’s IT staff.

Stage 2: Installing and configuring the components

Once the design is complete, the next stage is installing and configuring EMC Smarts components. This stage is usually broken down into deployment phases where related components are installed and configured together. Each installed and configured phase is validated individually as described in the next stage of the deployment process. This phased approach eases troubleshooting.

Many organizations have specific procedural requirements that must be met before and during installation of new software products in their production environments. These requirements might include lab installations with performance validations and pre-production deployments. Lab configurations usually require the use of a testbed that is configured and equipped similarly to the production environment. Acceptance tests may be performed before the deployment to the production environment. After the production deployment, the lab or testbed may be used to test upgrades and, if required, patches.

Though this guide cannot cover organization-specific requirements, it does provide guidelines that may aid you in responding to these conditions.

Installing and configuring the software is covered in “Deploying Service Assurance” on page 8-1. The deployment information, including software locations and all configuration choices, should be recorded in the Deployment Build Guide. Normally, this stage is performed by the purchaser of the deployment and either EMC Smarts Professional Services or an EMC Smarts partner.
Overview of the Service Assurance Deployment Process

Stage 3: Validating the deployment

Validating the deployment ensures that all installed components are operational and can communicate with each other as required and that the appropriate components can properly discover and poll the network.

Logical segments of EMC Smarts software are usually installed and validated to ease troubleshooting. Once all individual segments are installed and validated, the complete deployment must be validated from end to end. Included in this overall validation could be acceptance tests that demonstrate the functionality of the installation. Criteria for acceptance tests should be defined during the design stage. The execution of these acceptance tests and the results are usually included in an installation or build report.

Validating components is covered in “Validating Your Deployment (Acceptance Testing)” on page 9-1. Normally, this stage is performed by the purchaser of the deployment and either EMC Smarts Professional Services or an EMC Smarts partner.

Stage 4: Monitoring and tuning the deployment

Once EMC Smarts software is deployed and validated, you must ensure that it is operating at an optimal level. Tuning is the process of adjusting the configuration to improve performance; it should be performed after all components are installed and validated.

Note that this initial tuning process does not include rules writing or related maintenance: EMC Smarts software does not require this type of maintenance.

The process of monitoring a deployment for tuning is covered in “Monitoring the Performance of Your Deployment” on page 10-1. Normally, this stage is initially performed by either EMC Smarts Professional Services or a partner; and the knowledge is transferred to the purchasing organization’s staff. As the network and application infrastructure grows, the organization’s staff will take on the task of tuning the deployment to handle this growth. If the infrastructure growth is extensive, the original design may no longer be sufficient and redesigning the deployment may be required.

Through the life of the deployment, administrators should repeat this stage to maintain the deployment.
Before you begin checklist

Before you begin an EMC Smarts deployment, you must meet the requirements described in the following checklist. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

Table 1-1 Before you begin checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
</table>
| ❑ | Possess an understanding of the architecture and capabilities. | At a minimum, you must understand the concepts and architecture described in the following documents:  
  • EMC Smarts Service Assurance Manager Introduction  
  • EMC Smarts Service Assurance Manager Configuration Guide  
  • EMC Smarts Service Assurance Manager Adapter Platform User’s Guide  
  • EMC Smarts System Administration Guide  
  • EMC Smarts IP Management Suite Installation Guide that accompanied your product suite  
  • EMC Smarts user’s guides related to the underlying domains in your deployment.  
  
  To improve your understanding, attend training courses offered by EMC® Education Services and Development. Typically, deployment requires the knowledge equivalent to what is provided in the training courses on:  
  • Global Manager  
  • EMC Smarts Service Assurance Manager Adapter Platform  
  • Any underlying EMC Smarts domain that will be part of your deployment. |
| ❑ | Obtain contact information for the deployment team. | The contact list should include titles, responsibilities, and contact methods for all team members. |
| ❑ | Get non-disclosure requirements and negotiate an agreement. | Be aware of the requirements of the non-disclosure agreements that are in place for the deployment. |
| ❑ | Develop schedules and set milestones for early deliverable. | Scheduling a software deployment varies based on the size and scope of the deployment and the organization’s requirements. Typical milestones might include:  
  • Initial project meeting to define the deployment scope  
  • Purchase of EMC Smarts software  
  • Project development begins  
  • Installation in test environment complete  
  • Testing complete  
  • Installation in production environment complete  
  • EMC Smarts goes live  
  
  Additional information on scheduling is beyond the scope of this guide. |
This chapter describes the first step in designing a Service Assurance deployment: gathering the organizational and network-related information that is required to develop a successful design. This chapter also describes how to document the information that you gather and your resulting design in a Solution Architecture Diagram and a Deployment Build Guide. This chapter contains the following information:

- Document the deployment .......................................................... 2-2
- Determine the organization’s requirements ............................. 2-3
- Obtain network and application information .......................... 2-3
- Gather information required to size Service Assurance .......... 2-6
- Determine requirements for installing software .................... 2-8
- Define requirements for integrating existing software with EMC Smarts .... 2-8
- Gather network security information .................................. 2-9
- What other network features affect EMC Smarts? .............. 2-10
- Basic Service Assurance information checklist .................. 2-11
Document the deployment

The most useful way to document the managed environment and the design of your deployment is to create a Solution Architecture Diagram and record implementation details in a Deployment Build Guide.

The Solution Architecture Diagram

Based on the complexity of the deployment, a Solution Architecture Diagram may actually be a set of diagrams documenting various levels of the architecture.

The diagram relates the information that you gather on the environment to both physical and logical choices for your architecture in an easily understood manner. This diagram illustrates your design choices; and will be an important part of the review and approval process for your design.

The Solution Architecture Diagram should always include:

- Necessary information about the managed network and application environment
- A logical representation of the EMC Smarts components that will be installed
- Locations for each component including the name and IP address of the host and the geographical location of the host
- Connections between components and the ports that are used for communications
- Connections, including port numbers, between EMC Smarts components and external sources such as networks and third-party software products

This diagram cannot be completed until the design is complete and deployed, so recommendations for adding information to the diagram appear throughout this guide.

The Deployment Build Guide

To record the specifics of the managed environment and the deployment design and implementation, create a document called a Deployment Build Guide. As with the Solution Architecture Diagram, this chapter describes information that you should add to the Deployment Build Guide. The Deployment Build Guide should include the complete design and all installation specifications, validation results, and tuning activities.

Start the Deployment Build Guide by recording all the information that you gather on the network, some of which may come from your planning of IP Availability Manager or IP Performance Manager installations. As you continue the deployment process, this guide will include recommendations for adding other information to the Deployment Build Guide.
Determine the organization’s requirements

The design of an EMC Smarts deployment must support an organization’s needs. Most Requests for Information (RFIs), Requests for Proposal (RFPs), or Requests for Quote (RFQs) will begin with a description of the overall organization and its vertical market. Understanding the organization and its market can aid in making design choices.

The size of a company’s network and the amount of information monitored affects any implementation. Use an understanding of the business expectations in a vertical market to ensure a successful design. Typical vertical markets are listed in Table 2-1.

For example, each industry varies in the amount of downtime it can tolerate. As a general rule, financial organizations tolerate less downtime than organizations in the education vertical market. Most hosting service providers have more users monitoring network health than retailers.

Obtain network and application information

Gather information about the network and application and how they are utilized to accomplish an organization’s goals. A primary source for some of this information is an organization’s RFI, RFP, or RFQ for the deployment. The RFQ will normally contain details about important applications and about a network’s purpose, size, structure, and deployment needs.

Other sources of information include network diagrams and discussions with network and application administrators. If you can, include a copy of the network diagram that you obtain in the Build Guide.

Figure 2-1 on page 2-4 shows a typical network diagram that includes useful information for designing the Service Assurance deployment, such as the following:

- Physical geography of the network
- Locations of Network Operations Centers (NOCs)
- Lower speed WAN links such as T1 links
- Numbers of devices

This information appears in Figure 2-1 on page 2-4 in bold text.

<table>
<thead>
<tr>
<th>Typical vertical markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications</td>
</tr>
<tr>
<td>E-Business</td>
</tr>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Financial</td>
</tr>
<tr>
<td>General Business</td>
</tr>
<tr>
<td>Government/Defense</td>
</tr>
<tr>
<td>Health Care</td>
</tr>
<tr>
<td>Hosting Service Provider</td>
</tr>
<tr>
<td>Network Outsourcers</td>
</tr>
<tr>
<td>Retail</td>
</tr>
<tr>
<td>Transportation</td>
</tr>
<tr>
<td>Wireless</td>
</tr>
</tbody>
</table>
Gathering Basic Information

The network diagram may also include information that is important when designing underlying EMC Smarts domains, such as specific network device locations, ports, and interfaces used for connections, IP addresses, and names of network devices. This information is normally not needed for the Service Assurance design, but may be useful in ensuring that EMC Smarts components can connect across firewalls.
Determine network and application priorities

Organizations reflect their business priorities in their application and network organization. Certain priorities are more important and must be monitored more closely. It is highly likely that the Global Manager will have to monitor more information from the more important areas. The EMC Smarts applications may report more polling and threshold information, and there may even be other third-party applications producing information. All of this can affect sizing of the Global Manager.

Once again, the organization’s RFP should describe their needs and limitations.
Gather information required to size Service Assurance

To determine the size and configuration of Service Assurance, including the number of Global Managers and the equipment required to support them, gather the following information:

◆ The number of devices and applications to manage
◆ The number of Service Assurance clients
◆ The number of underlying managed domains

Determine how many devices and applications will be managed

One of the most important factors in determining the size of a Service Assurance deployment is quantity of devices and applications that must be managed. Count all managed devices in a network once. Include the following types of devices:

◆ All routers, including virtual routers
◆ All switches
◆ Hosts that will be managed
◆ Any other devices that will be managed

All managed applications should also be counted: if an application consists of component processes, count each process, also.

EMC Corporation has determined that even in well-managed large networks, administrators can underestimate the quantities of devices and applications that they intend to manage.

If possible, validate the estimated quantities for some portion of the network. If the estimate doesn’t match, try to obtain an improved estimate for another part of the network and then validate again. If improving the estimates is not possible, determine the percentage error and use it to adjust all the other estimates.

As a final step in estimating the quantities of managed devices and applications, account for growth of the organization’s network and for planned application deployments.

Your Service Assurance deployment design should account for network growth over the expected life of the design. The network growth rate will relate to the vertical market environment and the organization’s plans, so the organization must provide you with growth estimates.

Information on the future deployment of business applications may be more difficult to obtain. For example, an organization’s budgetary plans may provide useful information, but may not be available to you. Interviews with IT staff may be your best source of information.

Estimate quantities and types of Service Assurance clients

The number of Service Assurance clients will affect Global Manager configuration and equipment choices. The clients can include any of the following:

◆ Users of the Global Console, Web Console, and Business Impact Manager.
◆ EMC Smarts Adapters that connect to the Global Manager directly, including the Service Assurance Manager Notification Adapters: SNMP Trap Notifier Adapter, Script Notifier Adapter, and Log File Notifier Adapter.
Estimate the number of underlying EMC Smarts domains

Estimating the number of underlying domains requires that you size these domains following EMC Smarts Professional Services recommendations or by following the process described in the underlying domain’s deployment guide, such as the EMC Smarts IP Management Suite Discovery Guide.
Gathering Basic Information

Determine requirements for installing software

Most organizations define some criteria for installing new software on their network. At a minimum, this might include software testing requirements. In addition, plan on using a staging area before deploying. By staging the deployment, you can maintain a clean software distribution that does not include unwanted files, changes, and logs.

Define requirements for integrating existing software with EMC Smarts

Integrating third-party software products with EMC Smarts software requires the use of EMC Smarts adapters. Most integrations do one of the following:

- Exchange information. Determine the exact type of information (topology and/or events) that must be exchanged with any third-party software products.
- Allow access to the third-party software from the Global Console. Some EMC Smarts adapters provide this capability as the Server Tools functionality. For example, both the EMC Smarts Adapter for InfoVista and EMC Smarts Adapter for Concord eHealth allow users at the Global Console to access reports from these products.

EMC Corporation has developed many adapters for use with EMC Smarts software that may already support the integration requirements of your deployment. Itemize the integration requirements so that the suitability of existing EMC Smarts adapters can be assessed by EMC Smarts Professional Services. This guide specifically covers the integration capabilities provided by the EMC Smarts SNMP Trap Adapter (Receiver). This guide addresses the basic information for other adapters.
Gather network security information

Determine the level of security for the network that EMC Smarts software will monitor so that the software can be configured to a corresponding level of security. For example, the security needs of a network in a financial, defense, or health care vertical market may be greater than in the manufacturing vertical market. Enumerate security preferences, such as the use of passwords, encrypted password storage, and encrypted communications to guide you when configuring security capabilities.

Firewalls between parts of the EMC Smarts deployment

Appropriate Service Assurance components must be able to receive traps and communicate with other EMC Smarts components. Certain TCP and UDP ports will need to be opened in the firewalls to facilitate these communications. For more information, see “Considering security and firewalls” on page 3-12.
What other network features affect EMC Smarts?

Other network features may affect the EMC Smarts deployment design. Consider the following questions when gathering information on the network:

◆ Does the organization require failover capabilities in network software?

◆ Is there an “out-of-band” network just for management information? For example, are certain Ethernet ports just for management information? This is typical with some deployments in the financial and military/defense vertical markets.

◆ What are the issues related to network latency, bandwidth, and speed available for network management traffic?
Basic Service Assurance information checklist

Use the following checklist to aid in gathering information for your Service Assurance design. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

### Table 2-2  Service Assurance information checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Describe the organization’s requirements and expectations.</td>
<td>Document these requirements and expectations in the Deployment Build Guide.</td>
<td>“Determine the organization’s requirements” on page 2-3</td>
</tr>
<tr>
<td></td>
<td>Obtain network diagrams.</td>
<td>Ensure that the diagrams include the locations of the following:</td>
<td>“Obtain network and application information” on page 2-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The physical geography of the network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Locations of Network Operations Centers (NOCs)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lower speed WAN links such as T1 links</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Numbers of devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If possible, include the network diagrams in the Deployment Build Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describe the organization’s network and application priorities.</td>
<td>Document these priorities in the Deployment Build Guide.</td>
<td>“Determine network and application priorities” on page 2-5</td>
</tr>
<tr>
<td></td>
<td>Determine the number of managed devices and applications in the environment.</td>
<td>Document all quantities in the Deployment Build Guide.</td>
<td>“Determine how many devices and applications will be managed” on page 2-6</td>
</tr>
<tr>
<td></td>
<td>Estimate potential growth in quantity of managed devices.</td>
<td>The deployment must support potential network growth. Estimate the growth over a specific time period. Document the calculations in the Deployment Build Guide.</td>
<td>“Determine how many devices and applications will be managed” on page 2-6</td>
</tr>
<tr>
<td></td>
<td>Get the organization’s testing/acceptance requirements.</td>
<td>Your design may be required to meet test and acceptance requirements. Obtain any specifications that cover integration testing, user acceptance testing, and operational acceptance testing. You may be required to write an installation or deployment report that follows an organization’s particular standards.</td>
<td>“Determine requirements for installing software” on page 2-8</td>
</tr>
<tr>
<td></td>
<td>Describe the organization’s requirements for installing new software.</td>
<td>Document these requirements and how the design meets them in the Deployment Build Guide.</td>
<td>“Determine requirements for installing software” on page 2-8</td>
</tr>
</tbody>
</table>
### Gathering Basic Information

#### Table 2-2 Service Assurance information checklist (continued)

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>List the products that currently monitor the network and will be integrated with the EMC Smarts deployment.</td>
<td>Document the products (including version) in the Deployment Build Guide.</td>
<td>“Define requirements for integrating existing software with EMC Smarts” on page 2-8</td>
</tr>
<tr>
<td>✗</td>
<td>Describe the network security.</td>
<td>Describe security features that will affect the deployment. Document the security features in the Deployment Build Guide.</td>
<td>“Gather network security information” on page 2-9</td>
</tr>
<tr>
<td>✗</td>
<td>List any other network requirements or features that may affect the EMC Smarts deployment.</td>
<td>Document the features in the Deployment Build Guide.</td>
<td>“What other network features affect EMC Smarts?” on page 2-10</td>
</tr>
</tbody>
</table>
This chapter provides guidelines for producing an initial design of the Service Assurance deployment using the information you have gathered on the organization’s application and network environment. This chapter contains the following information:

- Determine the Service Assurance configuration ...................................................... 3-2
- Essential EMC Smarts applications ............................................................................ 3-9
- Locating the Global Managers in the network........................................................ 3-11
- Considering security and firewalls........................................................................... 3-12
- Considering failover (high availability) configurations ........................................ 3-13
- Designing acceptance tests ........................................................................................ 3-14
- Initial design checklist ................................................................................................ 3-15
Designing the Service Assurance Deployment

Determine the Service Assurance configuration

A single Global Manager can support most Service Assurance deployments, but there are cases where multiple Global Managers are required. Use Table 3-1 to determine the Service Assurance configuration required to support your managed environment. The first three columns in Table 3-1 identify the quantities that will determine the Service Assurance configuration:

- The Managed Devices and Applications column details the total quantity that will be managed in the Service Assurance deployment. This number should include estimates for growth.
- The Underlying Domains column details the total number of domains that will feed topology and events to the Service Assurance deployment.
- The Concurrently Connected Clients column details the total number of Service Assurance clients that will be connected concurrently, including Global Consoles, Web Consoles, Dashboard viewlets, and any adapters that connect to the Global Manager directly.

### Table 3-1 Determining the required Service Assurance configuration

<table>
<thead>
<tr>
<th>Managed devices and applications</th>
<th>Underlying domains</th>
<th>Concurrently connected clients</th>
<th>Global Manager configuration</th>
<th>Global Manager platform equipment tier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>≤10</td>
<td>≤100</td>
<td>Standard</td>
<td>Small</td>
</tr>
<tr>
<td>0 to 2,000 (small deployment)</td>
<td>&gt;100</td>
<td></td>
<td>Basic Hierarchical</td>
<td>Small Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Standard</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;100</td>
<td>Basic Hierarchical</td>
<td>Medium Medium</td>
</tr>
<tr>
<td>2,001 to 6,000 (medium deployment)</td>
<td>≤10</td>
<td>≤100</td>
<td>Standard</td>
<td>Small</td>
</tr>
<tr>
<td></td>
<td>&gt;100</td>
<td></td>
<td>Basic Hierarchical</td>
<td>Small Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≤100</td>
<td>Basic Hierarchical</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;100</td>
<td>Basic Hierarchical</td>
<td>Medium Medium</td>
</tr>
<tr>
<td>6,001 to 12,000 (large deployment)</td>
<td>≤10</td>
<td>≤100</td>
<td>Basic Hierarchical</td>
<td>Medium Medium</td>
</tr>
<tr>
<td></td>
<td>&gt;100</td>
<td></td>
<td>Hierarchical Presentation</td>
<td>Large All Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≤100</td>
<td>Hierarchical Presentation</td>
<td>All Medium Large</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;100</td>
<td>Hierarchical Mesh</td>
<td>All Large All Large</td>
</tr>
<tr>
<td>12,000 to 20,000 (extra large deployment)</td>
<td>≤10</td>
<td>≤100</td>
<td>Basic Hierarchical</td>
<td>Large Large</td>
</tr>
<tr>
<td></td>
<td>&gt;100</td>
<td></td>
<td>Hierarchical Presentation</td>
<td>Extra Large All Large</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≤100</td>
<td>Hierarchical Presentation</td>
<td>All Large Extra Large</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;100</td>
<td>Hierarchical Mesh</td>
<td>All Extra Large All Extra Large</td>
</tr>
</tbody>
</table>

Above 20,000 devices

EMC Smarts deployments in this range are currently in production. Consult with EMC Smarts Professional Services for aid in this design.
The Use This Service Assurance Configurations columns define recommendations to support the deployment:

- The Global Manager Configuration column details the recommendation for the number of Global Managers, either a single one (Standard) or multiple (any of the hierarchical configurations). If a hierarchical configuration is recommended, the specific structure is also defined. The Global Manager Configurations are explained in the following sections.

- The Global Manager Platform Equipment Tier columns define the hardware that is required to support the Global Managers. For hierarchical configurations, two layers of Global Managers are defined: an aggregation layer and a presentation layer. Domain Managers connect to a Global Manager at the aggregation layer while Service Assurance clients connect to a Global Manager at the presentation layer. The table indicates the equipment required to support each layer. The equipment tiers are defined in “Hardware for Service Assurance platform equipment tiers” on page 3-7.

Table 3-1 on page 3-2 defines Service Assurance configurations for coherent deployments. It is possible to create separate deployments in a managed environment that do not feed events and topology to a single, central Global Manager. If this is the case, each of these deployment must be treated separately with distinct Global Manager configurations based on unique quantities for first three columns in Table 3-1 on page 3-2.

---

**Standard Global Manager configuration**

A single Global Manager, as shown in Figure 3-1, should be able to handle many typical deployments. This is called the Standard Configuration. In this configuration, there are no links that introduce high latency between the main EMC Smarts components.

![Figure 3-1 Standard Service Assurance configuration](image)

**Basic hierarchical Global Manager configuration**

Deployments with either large numbers of clients and/or large numbers of domains can usually be supported using the Basic Hierarchical Configuration shown in
**Figure 3-2.** This hierarchical configuration separates the topology synchronization processing (aggregation) from the client processing (presentation) to improve performance.

Hierarchical aggragation Global Manager configuration

The Hierarchical Aggregation configuration shown in Figure 3-3 on page 3-5 uses multiple Global Managers at the aggregation layer to address these configurations:

- More than 10 underlying domains: EMC Corporation recommends that each Global Manager at the aggregation layer supports a maximum of 10 EMC Smarts domains. The example in Figure 3-3 on page 3-5, therefore, could support 20 domains.

- Geographically separate groups of domains: Using a standard Global Manager configuration would force some domains to connect to a Global Manager over a high-latency link. Additional Global Managers at the aggregation layer would be located in the same geographical area as the domains.

To ensure that acknowledgements and ownership of notifications are properly propagated, Service Assurance clients should only connect to the Global Manager at the presentation layer.
Hierarchical presentation Global Manager configuration

The Hierarchical Presentation Configuration shown in Figure 3-4 on page 3-6 uses multiple Global Managers at the presentation layer to address these configurations:

- More than 100 Service Assurance clients that connect concurrently: This includes Global Consoles, Web Consoles, Dashboard viewlets, and any adapters that connect to the Global Manager directly. EMC Corporation recommends that each Global Manager at the presentation layer support up to 100 concurrently connected clients, so the example in Figure 3-4 on page 3-6 would support 200 clients.

- Geographically separate groups of clients: In these cases, using a standard Global Manager configuration would force a group of clients to connect to a Global Manager over a high-latency link. Additional Global Managers at the presentation layer would be located in the same geographical area as the groups of clients.

To ensure that acknowledgements and ownership of notifications are properly propagated, some customization may be required.
Hierarchical Mesh Global Manager configuration

The Hierarchical Mesh Configuration shown in Figure 3-5 on page 3-7 is used to support the largest, most complex deployments that require multiple Presentation Global Managers and multiple Aggregation Global Managers.

As with the other hierarchical configurations, EMC Corporation recommends that each additional Aggregation Global Manager should support up to 10 underlying domains and each additional Presentation Global Manager should support up to 100 simultaneously connected clients.

Deploying the Hierarchical Mesh Configuration requires the aid of EMC Smarts Professional Services.
Designing the Service Assurance Deployment

Figure 3-5  Hierarchical Mesh Service Assurance configuration

Hardware for Service Assurance platform equipment tiers

Typical hardware for the equipment tiers and operating systems is listed in Table 3-2.

Table 3-2  Typical hardware for the equipment tiers

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Small (1-2 low end CPUs, 1 GB RAM)</th>
<th>Medium (2 CPUs, 2 GB RAM)</th>
<th>Large (2 CPUs, 4 GB RAM)</th>
<th>Extra large (4 CPUs, 8 GB RAM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>SunFire V210 or V240 (preferred)</td>
<td>SunFire V240 (fastest available)</td>
<td>SunFire V240 (fastest available)</td>
<td>SunFire V490 (fastest available)</td>
</tr>
<tr>
<td>HP-UX</td>
<td>HP rp3410-2, rp3440-4, rp4410-4, rp4480-8 (number means the amount of processors)</td>
<td>HP rp7420-16, rp8420-32</td>
<td>HP Superdome (from 16-64 processors)</td>
<td>HP Superdome (from 16-64 processors)</td>
</tr>
<tr>
<td>Linux</td>
<td>Any vendor, 1-2 Xeon 2.0GHz</td>
<td>Any vendor, 2 Xeon 3.0 GHz</td>
<td>Any vendor, 2 Xeon 3.6 GHz</td>
<td>Any vendor, 4 Xeon 3.6 GHz</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note: Some Windows 2003 and Linux configurations have been tested with VMware ESX Server. See the list of supported hardware/operating systems in the Installation Guides for your specific EMC Smarts product suites or contact EMC Smarts Global Services for the latest hardware equipment specifications.

Deploying Global Managers and Domain Managers

Deploy the Global Manager separately from the Domain Managers. Once deployments become large, run the Service Assurance Adapter Platform separately from the Global Manager. Avoid running any other applications on these platforms to ensure that you do not adversely affect the performance of the EMC Smarts applications.

Adding information to the Solution Architecture Diagram and Build Guide

Include the Global Managers and related applications on the Architecture Solution Diagram. Draw boxes to show the platforms and include the names, locations, and, when applicable, port numbers for the all EMC Smarts components.

For the Deployment Build Guide, document equipment choices and start a table that documents EMC Smarts components on each host.
Every EMC Smarts installation must include an EMC Smarts Broker and a license server. Both are critical components; without either, the installation will not work. Usually, you install these two components together, in a single location. All of the EMC Smarts applications must be able to communicate with both applications.

Locating EMC Smarts Brokers

The Broker manages a registry of EMC Smarts server applications. When an EMC Smarts application needs to connect with another application, it gets the necessary information from the Broker. Periodically, the Broker pings the applications in its registry to determine whether they are still active.

Server applications, such as the Global Manager, IP Availability Manager, and Adapter Platform, are maintained in the Broker’s registry. Applications such as the Global Console connect to the Broker to determine the location of registered applications.

With most installations, the Broker is typically installed on the same machine as the license server. All EMC Smarts applications must be able to access the Broker. By default, the Broker uses port 426.

EMC Corporation recommends that you use a DNS alias to a machine for the Broker (smarts-broker) so that it is easier to redirect other EMC Smarts applications if it becomes necessary to move.

Add the following information for the Broker to the Deployment Build Guide:

- Name of host where the Broker will reside
- Port number to be used by the Broker (The default is 426.)
- Information for the DNS broker alias

Installations use more than one Broker for failover configurations. Multiple Brokers require special consideration to synchronize lists of registered servers. If you determine that your installation needs more than one Broker, consult with the EMC Smarts Professional Services organization.

Locating license servers

The license servers authenticate EMC Smarts applications. Without the proper licensing, the applications will not work correctly. Licenses control access to applications and features as well as limit the number of systems discovered.

EMC Corporation recommends that the license server run on the same host as the Broker—all applications need to be able to access the license server. However, an existing FLEXnet License Server may be used if it meets the EMC Smarts specifications. If there is more than one Broker for the installation, there may be good reason to use more than one license server.

In certain cases, you may use multiple license servers in your network for the same reasons that you split a topology or choose different locations for the Domain Managers: geographical requirements, corporate organizational requirements, or the network’s security design. Using multiple license servers requires the corresponding number of licenses.
Designing the Service Assurance Deployment

When multiple license servers are used, each domain will use blocks of licenses from a specific license server. Therefore, the license blocks must be divided among multiple licenses and the appropriate license must be deployed to each license server. Then, the Domain Managers that rely on a specific license server will have the appropriate licenses to support the systems that they must manage.

Collect the following information for each license server and add it to the Deployment Build Guide:

◆ The host ID of the computer where the FLEXnet license server is running
◆ The expected installation path to BASEDIR/smarts/bin on your broker (or to the EMC Smarts installation from which you want to run the license server)
◆ The operating system of the computer
◆ The port number used

For more information about licensing, see EMC Smarts System Administration Guide.
Locating the Global Managers in the network

In choosing locations for the platforms that support the Global Managers, there may be restrictions on locations that are not related to network and application efficiency. Locating the Global Managers may be based on the following considerations:

- Geographical requirements: An organization may require that all EMC Smarts Managers be based in a single Network Operations Center (NOC). Other organizations might have the Global Manager in the NOC and underlying Domain Managers located in regional data centers.

- Corporate organizational requirements: For example, organizations that have a distributed business management might require that components be located to match the organization’s structure.

Communication between applications is influenced by network speed and latency. Avoid configurations that require a Global Manager to receive information from other applications across WAN links with high latency. Instead, consider placing Global Managers on both ends of high-latency WAN links. The hierarchical Global Manager configurations can be used to eliminate high-latency link issues for these situations:

- Domain Managers that connect to a Global Manager over a high-latency link: Use the basic hierarchical, hierarchical aggregation, or hierarchical mesh configuration to place a Global Manager on the same side of the high-latency link as the Domain Managers.

- A group of clients that connect to a Global Manager over a high-latency link: Use the basic hierarchical, hierarchical presentation, or hierarchical mesh configuration to place a Global Manager on the same side of the high-latency link as the group of clients.

After you determine the configuration and locations of the Global Managers, add system names and Global Manager names to your Solution Architecture Diagram. Define IP addresses and dedicated port numbers when needed. Establish a host naming convention and a Global Manager naming convention before you settle on any names.
Considering security and firewalls

Based on the security information you obtained earlier, you must plan design solutions so that the applications can function properly in the network’s security environment:

- Configure security policies (rules) to enable a one-way connection from the FLEXnet license server and the Broker to the various applications.

  For communication between Smarts Managers across firewalls, plan on opening a hole in the firewall for the EMC Smarts communications. Certain UDP and TCP ports must be opened for proper communications:
  
  - Broker: Port 426
  - License Manager: Port 1744
  - Smarts Manager: one port each, which can be configured.
  - Adapters, including SNMP Trap Adapter and Syslog Adapter: See EMC Smarts Service Assurance Manager Adapter Platform User’s Guide for more information.

- Consider proxy servers when communicating with EMC Smarts applications that reside behind firewalls. Using a proxy server reduces the number of firewall ports that need to be opened to one firewall port. See “Configuring the Java clients to use a proxy server” on page 8-5.

- If access lists are used, plan on deploying the IP addresses of hosts that include Smarts Managers to the access list of devices that will be managed. EMC Smarts applications must have full access to browse the MIBs of the devices. (The specific MIBs are listed in the EMC Smarts IP Availability Manager User’s Guide and the EMC Smarts IP Performance Manager and Server Performance Manager User’s Guide.) Depending on the network size and complexity, this may require scheduling to obtain support from the organization’s network personnel.

- You must have a listing of SNMP versions and related security parameter values that are used by specific devices in the organization’s network. Due to security concerns, it may not be appropriate to include them in the Deployment Build Guide.

Security levels and EMC Smarts applications

In addition, consider the level of security to configure for EMC Smarts applications. The security mechanisms support various levels of user authentication, and authentication and encrypted communication between applications. Ensure that you understand the capabilities described in the EMC Smarts System Administration Guide and then choose a level of security that is appropriate for the deployment.
Considering failover (high availability) configurations

EMC Smarts offers a failover product that works in conjunction with the Global Manager. You can find information about configuring a failover solution in the EMC Smarts Service Assurance Manager Failover System User’s Guide. For additional help, consult with EMC Smarts Professional Services.
Designing acceptance tests

Acceptance tests may be required for different portions of EMC Smarts functionality. Be aware of the requirements and develop acceptance criteria with the aid of the network administrators and other organization personnel. Include all necessary acceptance tests in the Deployment Build Guide for the deployment. At a minimum, you must develop completion criteria that the organization’s project managers approve. Document these completion criteria in the Deployment Build Guide and use them in validation.
Document your initial overall design of the deployment.

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑</td>
<td>Determine the configuration of the Service Assurance Deployment.</td>
<td>Determine Service Assurance configuration, including the number of Global Managers and how they are organized in the deployment.</td>
<td>“Determine the Service Assurance configuration” on page 3-2</td>
</tr>
<tr>
<td>❑</td>
<td>Determine the hardware required to support the Service Assurance Deployment.</td>
<td>For each Global Manager in the Service Assurance configuration, determine the type of equipment required to support it.</td>
<td>“Hardware for Service Assurance platform equipment tiers” on page 3-7</td>
</tr>
<tr>
<td>❑</td>
<td>Determine the location of the EMC Smarts Broker.</td>
<td>Choose a location for the Broker that will support the deployment.</td>
<td>“Locating EMC Smarts Brokers” on page 3-9</td>
</tr>
<tr>
<td>❑</td>
<td>Determine the location of the License Server.</td>
<td>Choose a location for the License Server that will support the deployment.</td>
<td>“Locating license servers” on page 3-9</td>
</tr>
<tr>
<td>❑</td>
<td>Determine the location of the EMC Smarts Global Manager(s).</td>
<td>Choose locations for the one or more Global Managers that will support the deployment.</td>
<td>“Locating the Global Managers in the network” on page 3-11</td>
</tr>
<tr>
<td>❑</td>
<td>Determine if the Service Assurance Manager must be configured with failover.</td>
<td>Determine if a high-availability configuration is required.</td>
<td>“Considering failover (high availability) configurations” on page 3-13</td>
</tr>
<tr>
<td>❑</td>
<td>Determine if acceptance tests are required.</td>
<td>Acceptance tests may be required for different portions of functionality. Be aware of the requirements and develop acceptance criteria.</td>
<td>“Designing acceptance tests” on page 3-14</td>
</tr>
</tbody>
</table>
This chapter describes considerations for importing and organizing topology. Additional details about the methods for importing and organizing topology are found in the *EMC Smarts Service Assurance Manager Configuration Guide*.

This chapter contains the following information:

- Designing topology synchronization ................................................................. 4-2
- Designing topology groupings ........................................................................... 4-4
- Designing topology operations checklist ........................................................... 4-5

**Note:** For business and application topology, see the *EMC Smarts Business Impact Manager User’s Guide* and the *EMC Smarts Application Services Manager Discovery Guide*. 
Designing topology synchronization

A Global Manager imports topology from certain types of underlying EMC Smarts domains. The topology sources are specified in the Global Manager’s ics-default.xml file. A Global Manager synchronizes its topology whenever any of the following occurs:

◆ The Global Manager is started.
◆ A change is made to the DomainType section of the Global Manager’s ics-default.xml file.
◆ The analysis domain is reconnected after a connection loss or a restart.
◆ The analysis domain performs a full or incremental discovery, or redisCOVERS an object; or a manual discovery is initiated.

Understanding topology synchronization

The Global Manager maintains an abstracted representation of the topology discovered by the Domain Managers and the topology from the Adapter Platform. When the Domain Manager completes a discovery, the Global Manager resynchronizes the topology from the Domain Managers.

In all cases, the Global Manager does a full topology synchronization, even when only one device is added to an underlying domain. This means that topology synchronization is most efficient when it occurs less frequently, but with larger sets of changed devices. The Global Manager resynchronizes topology after a single device discovery, a pending discovery, or a full rediscovery.

Another important aspect of topology synchronization is synchronization between the Global Manager and the Adapter Platform. The Adapter Platform is typically configured to contain some of the topology from the IP Availability Manager. With this topology, the Adapter Platform matches events to devices managed in the IP Availability Manager. So, the Adapter Platform often contains all of the IP Availability Manager topology and also some topology created based on events received as traps, or from other sources.

When the Global Manager synchronizes topology with the Adapter Platform, the topology inherited from the IP Availability Manager, as well as the topology created due to events from traps or other sources, is synchronized. This means that a Global Manager may synchronize topology twice when a change is made to a device in IP Availability Manager: once with the IP Availability Manager and then once with the Adapter Platform.

Because the Adapter Platform does not contain all of the topology from the IP Availability Manager, the synchronization it performs with the Global Manager for the topology from IP Availability Manager is less performance-intensive than the synchronization between the Global Manager and the IP Availability Manager.

Topology synchronizations in the Global Manager may be done concurrently. If there are a number of underlying domains that need to synchronize topology at the same time, the Global Manager may synchronize these at the same time. In most cases, this gives optimal performance. However, if there are many concurrent topology synchronizations, the performance of the Global Manager may be adversely affected. Also, topology synchronizations overall may take longer due to the contention caused by many concurrent threads updating the Global Manager repository.
Planning for topology synchronization

If there are a large number of underlying domains and the topology of each changes frequently, it is likely that the Global Manager will often be required to perform multiple concurrent topology synchronizations.

To optimize Global Manager performance, it is best to reduce the number of small discoveries, and instead have a smaller number of larger discoveries. Also, if full re-discoveries are scheduled, Global Manager performance can be improved by staggering the times of full rediscoveries of the underlying domains.

Finally, if you expect a constantly changing network with a large number of discoveries, you may want to reconsider your Global Manager configuration. If you are not already planning on implementing a hierarchical aggregation Global Manager configuration or hierarchical mesh Global Manager configuration, consider using one of these configurations (see “Determine the Service Assurance configuration” on page 3-2).
Designing topology groupings

Topology grouping is a visual tool that does not affect Global Manager performance. Groups help organize topology elements. The groups can represent resources, geographic areas, business areas, or other organizations entities.

Think about groups in terms of the business needs: Is your topology divided by region? Does the topology correspond to business units? Is the topology allocated by customer or function?

Groups are organized into parent and child groups. A group can contain both members and child groups. When planning group organization, you should try to restrict each group to hold only members or only child groups. The Map Console will not show the members of a group if the group also contains child groups.

There are two ways to create groups. The first method uses matching patterns entered through a Global Console. This method creates selective groups. The second method relies on a file to determine group hierarchy and membership. This method creates hierarchical groups.

For selective groups, you must define three properties to organize your groups: matching criteria, priority, and target classes. You define hierarchical groups and their members using files. One file contains groups and child groups, which can also include members or links to files that contain members.

For more information about topology groupings, see EMC Smarts Service Assurance Manager Configuration Guide.
Designing topology operations checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

Table 4-1  Designing topology operations checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Review topology synchronization</td>
<td>Ensure that you understand how topology synchronization affects Global Manager performance.</td>
<td>“Understanding topology synchronization” on page 4-2</td>
</tr>
<tr>
<td>✔️</td>
<td>Plan topology synchronizations</td>
<td>To optimize Global Manager performance, it is best to reduce the number of topology synchronizations where possible.</td>
<td>“Planning for topology synchronization” on page 4-3</td>
</tr>
<tr>
<td>✔️</td>
<td>Plan topology groups</td>
<td>Topology grouping is a visual tool that does not affect Global Manager performance. Groups help organize topology elements.</td>
<td>“Designing topology groupings” on page 4-4</td>
</tr>
</tbody>
</table>
This chapter covers the basics of notification handling for the Global Manager, the Adapter Platform, and clients of the Global Manager. The design and deployment of notification handling is an iterative process. Start with a basic configuration and make adjustments based on results. The chapter contains the following information:

- Overview of notification processing .................................................. 5-2
- Designing trap processing ............................................................. 5-4
- Trap processing performance ......................................................... 5-7
- Planning for notifications checklist .................................................. 5-9
Overview of notification processing

In the typical configuration of the Global Manager, there are two types of information sources: the Adapter Platform, which handles information from third-party applications, and the underlying EMC Smarts Domain Managers. After the Global Manager processes the information, it forwards the results to end users through clients such as the Global Console or an adapter that sends information to third-party applications.

Figure 5-1 is an example of a basic Global Manager configuration. The lines show how information enters through either an IP Availability Manager (or other underlying Domain Managers) or an Adapter Platform, is passed to a Global Manager, and finally is passed to an end user or application. Note that the figure does not show the connection that transports topological information between the IP Availability Manager and the Adapter Platform.

The Adapter Platform imports topology and event information from third-party applications and prepares it for use by the Global Manager; data from third-party applications should not be sent directly to the Global Manager. The Adapter Platform creates notifications from the incoming information and can even associate these notifications to topology information supplied by another EMC Smarts application (this connection is not shown in Figure 5-1).

Efficient notification processing presents the most important information to the operator using a Global Console. One of the goals of deployment design is to plan to
optimize the flow of notifications sent through the system. This improves the performance of the deployment and the performance of the operators using EMC Smarts products.

Notifications from the Adapter Platform

Ensure that only the notifications that are useful to Global Console operators reach the Global Manager. When EMC Smarts software is first deployed, a strategy to reduce and control the flow of notifications from the Adapter Platform to the Global Manager temporarily is to prevent any notifications from the Adapter Platform from being forwarded to the Global Manager using notification list filtering. Use the Global Console to connect directly to the Adapter Platform and observe the notifications there; evaluate the notifications. Then, modify the notification list to forward useful notifications to the Global Manager.

Configuring notifications for clients

Notification Lists are the mechanism that clients use to subscribe to and receive notifications from a Global Manager. Smaller notification lists produce better performance in both the client and the Global Manager.

Notification Lists are associated with user profiles—one list per profile. When designing notification lists for consoles, attempt to design them so that they do not typically include more than 500 active notifications.

It is more efficient to prevent a notification from being sent to an EMC Smarts client using a notification list than to use a filter to remove the notification from the Notification Log view at a client’s console. These filters do not curtail the output of notification lists and do not provide any performance benefit to the Global Manager.

See “Designing notification lists” on page 6-5 for information about configuring clients to receive notifications.
Planning for Notifications

Designing trap processing

Any EMC Smarts deployment should include a plan to handle trap processing. This section covers one method.

Recommended trap processing design

EMC Corporation recommends the trap processing design in Figure 5-2 on page 5-5. This configuration relies on two instances of the SNMP Trap Adapter to handle trap processing and performs well under the stress of high volumes of traps.

Instance 1 of the adapter is configured as a trap exploder that receives and forwards traps. In this configuration, the trap exploder does not process traps into notifications or use any ASL scripts for sophisticated trap processing. The trap exploder’s sole function is to filter and forward traps as follows:

- IP Availability Manager-required traps are forwarded to IP Availability Managers.
- Traps required for other EMC Smarts domains are forwarded to the proper domain (not shown in Figure 5-2 on page 5-5).
- Other useful traps are forwarded to Instance 2 of the SNMP Trap Adapter for processing into notifications. These traps provide meaningful or actionable information to the administrators of the network.
- Traps may be received in SNMP v1, v2c, or v3 formats; however, they are forwarded on to the Adapter Platform or to other Domain Managers as SNMP v1 or v2c only.
- Other traps that administrators do not consider useful can be forwarded to an unused port to reduce overhead at the SNMP Trap Adapter. Normally, the adapter logs an error message for each trap that is not forwarded. This practice eliminates the processing associated with error message logging. Another benefit is that forwarding these traps to a location permits you to set up a tool to collect the traps.

Instance 2 of the SNMP Trap Adapter performs the typical processing of traps into notifications and may invoke ASL scripts for advanced processing. This instance does not forward any traps.

The two SNMP Trap Adapter instances are invoked using different configurations. The typical configuration when the instances are on a single host is the following:

- The trap exploder, Instance 1 of the SNMP Trap Adapter, uses BASEDIR/smarts/local/conf/trapd/trapd.conf. This trapd.conf file includes trap forwarding statements and indicates the port to use when listening for traps.
- Instance 2 of the SNMP Trap Adapter processes traps into notifications and uses InCharge7/SAM/smarts/local/conf/icoi/trapd.conf and InCharge7/SAM/smarts/local/conf/icoi/trap_mgr.conf. This instance of the trapd.conf file does not include trap forwarding statements. (If the Trap Adapter was installed as a service, these traps will be forwarded to the Adapter Platform by default). The trap_mgr.conf file includes definitions for all traps that will be forwarded as notifications.
Note: The trapd.conf files installed with IP Availability Manager and IP Performance Manager can be configured to permit the IP Availability Manager and the IP Performance Manager to forward traps using their built-in trap receivers. This capability should not be used except for testing deployments or when migrating traps from multiple locations to one destination.

For a complete description of the SNMP Trap Adapter see the EMC Smarts Service Assurance Manager Adapter Platform User's Guide.

![Diagram of recommended trap processing design](image)

**Figure 5-2 Recommended trap processing design**

**Batching to improve performance**

In a deployment where a high frequency of traps is expected, plan on using the batching capability of the SNMP Trap Adapter to improve performance of clients that process the notifications. The BATCH_NOTIFY_INTERVAL in the trap_mgr.conf configuration file determines the length of the interval. It may be necessary to fine tune this value under the typical trap load, so plan on monitoring the client performance and adjusting this value.
Planning for Notifications

Listening for traps

The SNMP Trap Adapter configured as the trap exploder should listen for traps on the standard port that network devices use when forwarding traps. Typically, this is port 162.

If another application is listening for traps at this port, the application should be moved and the trap exploder can forward needed traps to the application’s new location. The SNMP Trap Adapter is usually a better choice for forwarding traps than other third-party software applications because the adapter can be limited to the forwarding function.

The second instance of the SNMP Trap Adapter can listen on any port, but the trap exploder must be configured to forward the appropriate traps to this port.

Trap forwarding

When defining trap forwarding, traps required by underlying EMC Smarts domains are already defined in the trapd.conf file. The only change that you must configure is to specify the specific destination hosts and ports where the domains listen for traps. This change is only necessary in the BASEDIR/smarts/local/conf/trapd/trapd.conf file for the trap exploder instance of the SNMP Trap Adapter (Receiver).

Always try to minimize the volume of traps that are forwarded from the trap exploder to the second instance of the SNMP Trap Adapter. If network administrators do not use the traps, discard them by sending them to a nonexistent address. Judicious forwarding of traps can reduce or eliminate stressful trap processing loads. Deployment administrators should be aware of how traps are discarded so that they can choose to discard other useless traps as their experience with the network grows.

Each trap that is transformed into a notification will require an entry in the trap_mgr.conf file. If an entry does not exist, the trap should not be forwarded to the second instance of the SNMP Trap Adapter.

Traps and notifications

When configuring the SNMP Trap Adapter to process traps, you must decide which traps should become notifications and how the notifications should appear at the Global Console. This is defined in the trap_mgr.conf configuration file which is described in the EMC Smarts Service Assurance Manager Adapter Platform User’s Guide.

Advanced trap processing using ASL scripts

See the EMC Smarts Service Assurance Manager Adapter Platform User’s Guide for specific information on advanced SNMP Trap Integration. Typically, the ASL scripts (hook scripts) will extract event text or other important information from network sources to populate the User Defined fields in the notification.

Include as much of the ASL processing definition as possible in the Deployment Build Guide. When the ASL scripts are complete, the code should be documented in the Deployment Build Guide.
Trap processing performance

The following processing issues impact performance directly:

- Filtering traps in trap_mgr.conf
- Using trap manager hook scripts
- Adding new topology for received traps
- Looking up host names
- Batching traps

Consider them as you design and configure trap processing in your environment.

Filtering traps in trap_mgr.conf

The number of traps that are processed and specified in trap_mgr.conf is a factor in performance. The smaller the number of received traps processed as events, the higher the overall rate of processing.

With trap receiver you can import subsets of traps into the Adapter Platform. Large numbers of traps may be sent by network devices, but typically only a small subset are important to network operators. For example, link up and down traps are sent frequently by devices but are not typically important to display to the network operator since the Availability Manager already supplies authentic, root-cause problems related to these traps.

Using trap manager hook scripts

With the trap manager, you can customize trap processing by using an ASL hook script. Typically, this additional processing causes performance to be slightly slower than if no ASL hook scripts are used.

Adding new topology for received traps

The trap manager allows the Adapter Platform to create a topology element if a trap is received for an element that is not already in the topology. The performance declines whenever a large percentage of the traps processed result in topology creation and increases whenever all traps relate to existing topological elements.

Looking up host names

The trap processing logic may require a reverse host name lookup to find the logical name of the element sending a trap based on the IP address. The speed of this host name lookup in a particular customer’s environment may have a significant impact on trap processing rates. For example, if a customer uses a DNS host lookup and a large number of traps are received for devices not listed in DNS, DNS time-outs may significantly impact trap processing performance.

Batching traps

Configuring the trap manager to batch traps for the same notification results in improved performance due to the reduced number of notifications and updates that need to be processed.
The trap manager has an option to batch traps whenever multiple traps for the same notification are received within a configurable number of seconds. For example, if 50 identical traps are received from a single device in 2 seconds, the result is 50 updates to the same notification. All clients receiving these notifications would receive 50 updates to the notification. Setting a two-second batch interval, however, means that there is only one update to the notification, even though 50 traps were sent.
Planning for notifications checklist

Before discovering the network, the requirements in the following checklist must be completed. Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

Table 5-1  Planning for notifications checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Determine which notifications are important for EMC Smarts operators.</td>
<td>Ensure that only the notifications that are useful to Global Console operators reach the Global Manager.</td>
<td>“Overview of notification processing” on page 5-2</td>
</tr>
<tr>
<td></td>
<td>Configure Notification Lists.</td>
<td>Notification lists are the mechanism that clients use to subscribe to and receive notifications from a Global Manager.</td>
<td>“Configuring notifications for clients” on page 5-3</td>
</tr>
<tr>
<td></td>
<td>Design Trap Processing.</td>
<td>Any EMC Smarts deployment should include a plan to handle trap processing.</td>
<td>“Recommended trap processing design” on page 5-4</td>
</tr>
</tbody>
</table>
This chapter describes how best to use EMC Smarts clients to satisfy the needs of operators, including providing appropriate access rights to monitoring and administration functions. This chapter contains the following information:

- Who are the Global Manager users? ........................................................................... 6-2
- Choose a console for types of users ............................................................................ 6-3
- Designing user profiles ................................................................................................. 6-5
- EMC Smarts user design checklist .............................................................................. 6-7
Who are the Global Manager users?

When designing your deployment, you must determine who will use the Global Consoles and for what purposes. Initially, it is not necessary to define individual users—consider, instead, broad functional categories of users with similar needs and characteristics.

Name these categories of users, and list their requirements in the Deployment Build Guide. Using specific position names as categories can make the process easier. For example, you might create one or more of these categories: application engineer, application administrator, application support specialist, network engineer, network administrator, network support specialist, NOC manager, NOC operator, LAN administrator, and IT management. Once you choose categories, determine the typical EMC Smarts-related duties that are performed by the individuals in these categories. You may find that as you list the duties, you have to expand or combine certain categories. Once the categories are completely defined, list them and their specific needs in the Deployment Build Guide.

For example, Table 6-1 defines two typical user categories.

<table>
<thead>
<tr>
<th>User Category</th>
<th>Description of Needs/Duties</th>
</tr>
</thead>
</table>
| Network Engineer | Administers and maintains local and wide area networks and related hardware. Monitors daily activity, enforces licensing agreements, and provides front line support, including both software and hardware support.  
  • Needs monitoring access to all EMC Smarts domains.  
  • Needs to see all important traps, notifications, and network outages. |
| Local Area Network Administrator supporting a Customer of a Service Provider | Directs the daily operational availability of the hardware and software systems required to support facility operations. Directs and oversees scheduled testing and review of hardware and software to ensure that potential problems are identified as soon as possible. Analyzes, evaluates, and builds cost effective LAN solutions that leverage resources and technology to meet business requirements. Designs, creates, and distributes user documentation relating to installation of software.  
  • Needs monitoring access to the EMC Smarts domain that supports the customer, but not access any other domains.  
  • Needs to see all important traps, notifications, and network outages for the customer’s EMC Smarts domain. |
Choose a console for types of users

EMC Smarts consoles have different capabilities. For each type of user and their equipment, determine which console is most appropriate:

- Global Console can provide all functions and all views to operators. Administrators can restrict console operations so that operators have only the specific functionality that they require.
- Web Console can also provide all functions and all views that are available from the Global Console, except for the Topology Browser Console. As with the Global Console, most console operations can be restricted.
- Business Dashboard provides access to the results of EMC Smarts analysis via one or more Dashboard viewlets implemented as Java applets. A Dashboard viewlet is a Java application that shows a particular aspect of Service Assurance information such as notifications, containment, or maps. Dashboard viewlets provide operational functions, but no administrative functions.

A Global Console, a Web Console, and a Business Dashboard (on a single browser using one Java Virtual Machine) showing similar content, all use the same resources. This is regardless of the number of viewlets displayed by the Business Dashboard.

Deployment considerations for client consoles

Each of the available Client Consoles has different deployment considerations. Typically, the Global Console is deployed by installing EMC Smarts software on the user’s system, but the Global Console can also be accessed using the X Windows server software on the user’s system when the Global Console runs on a remote UNIX server. If using X Windows, the client that displays the application over X does not require Java.

The Web Console can be deployed in two ways:

- As a typical Java applet where the HTML and JAR files are located on the host where the Business Dashboard is installed. When a user opens the Web Console, the JAR files are loaded over the network to the user’s Web browser.
- Using Java Web Start, which integrates the Web Console with the user’s desktop. This enables users to start the Web Console directly from their desktop without using a Web browser.

With both methods, the JAR files are loaded over the network during the initial connection but then saved to the user’s local system. Subsequent connections use the cached files to optimize the use of network resources.

An installation of the Business Dashboard includes the Tomcat Servlet Engine, which is necessary to serve the JAR files and map layout servlet. The servlet engine is installed as the EMC Smarts Servlet Engine service on the system where you install the Business Dashboard. If you wish to serve Dashboard viewlets from a different Web server, you must install the Business Dashboard to obtain the necessary files.
Users and security

When defining the functional categories for users, consider the EMC Smarts security implementation. For each user category, determine the following:

- List the specific EMC Smarts managers that must be accessed by the users in the category. If necessary, divide a category. For example, in a category of Network Administrators, some users require access to managers in Asia, other users require access to managers in Europe, and still other users require access to all managers. In this case, the Network Administrators category could be divided into three categories to match these user needs while maintaining tighter security.

- Determine what functionality must be accessed by users in this category. EMC Smarts software is designed so that users can be classified into levels that define access:
  - All, a level where users can access all Global Console functionality available for one or more EMC Smarts Managers, if their user profile permits it.
  - Monitor, a level where users can access only Global Console monitoring functionality, not administrative functionality, at one or more EMC Smarts Managers, if their user profile permits it.
  - Ping, a level normally reserved for EMC Smarts processes, where processes will ping hosts where other EMC Smarts processes are installed to determine if the hosts are running.
  - None, a level that specifically excludes access to the Global Console.

These types of security access are defined in the `serverConnect.conf` file on the servers where EMC Smarts software is installed.

Password configurations

Determine how you will configure EMC Smarts passwords. You can do any or all of the following:

- Allow the host operating system to validate users. This method provides the highest level of security and is easy to manage because it relies on the security implementation that is already in place. There are two variations: Any valid user can access one of the EMC Smarts levels (All, Monitor, Ping), or specific users can access a specific EMC Smarts security level. Defining specific access requires more maintenance because you must list the user names in the configuration files (serverConnect.conf and clientConnect.conf). See the EMC Smarts System Administration Guide for methods to configure and to secure access for these files.

- Specify unique passwords for individual users. Consider this method only when there are very few users because it requires a high level of maintenance. Note that it is less secure than permitting the host to validate users. Plan on using the EMC Smarts password encryption mechanism described in the EMC Smarts System Administration Guide.

- Specify a common user name with a common password. This method is the least secure, but very easy to maintain. Plan on using the password encryption mechanism described in EMC Smarts System Administration Guide.

Note that you can combine these methods, for example, you could restrict administration (All) capabilities to specific users validated by the operating system. In addition, you could provide Monitor level abilities to a general EMC Smarts user named “Monitor.”
Designing user profiles

The functional grouping of users and their requirements form the basis of EMC Smarts user profiles. These profiles combine access to Notification Lists, console operations, custom console layouts, and specific tools.

Create a profile for each category of user that you must support. Groups of users with similar needs can then be assigned the same user profile.

If needed, you can further customize a generic user profile by copying it and then modifying it for more specific needs. For example, an administration user profile could be customized for less experienced administrators by restricting access to some administrative console operations and tools. Other possible user profiles could include regional or customer-specific consoles.

Designing notification lists

A Notification List determines the events that are forwarded to a user. Essentially, the list filters the notifications that are sent from the Global Manager and can be assigned to one or more users. The lists can be organized by:

- Business units
- Geographical regions
- Groups of resources

For example, a Notification List can be defined to allow only notifications from the subnetworks devoted to a specific ISP customer to reach the Global Console of the customer’s network administrator. See “Configuring notifications for clients” on page 5-3 for more information.

Restricting console operations

Most operations that can be performed at the Global Console can be individually enabled or disabled in the user profiles. When used with the security levels, restricting console operations can fine tune user access to functionality and further protect the deployment.

For example, consider two users who have the Monitor security level that allows access to Global Console monitoring functionality, but not administrative functionality, for an EMC Smarts Manager. You can further restrict one of the viewers to see only the Summary view and the IP Network Map while restricting the other user to the Notification Log and the Topology Browser.

Designing consoles

Specific console layouts can be saved and then automatically provided to match user needs at the Global Console, Web Console, and Business Dashboard. Layouts including the Notification Log view, Map view, Summary view, Status Table view, Notification Properties view, and Containment view can be used to create a custom console layout for Global Console and Web Console users. These same views can be provided to Business Dashboard users as Dashboard viewlets. Another view, the Topology Browser view, can only be used in layouts for Global Console and Web Console users.
Filtering the Notification Log view at the Global Console or Web Console does not affect Global Manager performance, but it can be used to create a simpler, more useful Notification Log view for groups of users. Properly configured filters can be used to customize notification consoles for groups of users. In addition, specific views can be automatically provided to match user needs.

Topology Browser views (not Map views) are more resource intensive than others. Carefully consider the information that operators require before including the Topology Browser view in a console layout.

All console layouts are created using the Global Console and then deployed by copying them to appropriate directories on the Global Manager.

Planning for tools and tool deployment

Many types of client and server tools can be designed and developed for users. Typically, creating tools will require different levels of programming skills based on their complexity. Plan to have individuals with the appropriate skills available to create the tools. In addition, determine which tools should be available to which users through their user profiles.
# EMC Smarts user design checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are all grouped together in “Design and Deployment Checklists” on page A-1.

## Table 6-2  Client and user design checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Define functional groups for users.</td>
<td>List the broad functional groups that users will belong to and then define the needs and duties of each group. Add this information to the Deployment Build Guide.</td>
<td>“Who are the Global Manager users?” on page 6-2</td>
</tr>
<tr>
<td></td>
<td>Choose appropriate EMC Smarts clients for users.</td>
<td>EMC Smarts consoles have different capabilities. For each type of user and their equipment, you must determine which console is most appropriate. Document your choices in the Deployment Build Guide.</td>
<td>“Choose a console for types of users” on page 6-3</td>
</tr>
<tr>
<td></td>
<td>Define how you will implement security for user groups.</td>
<td>When defining the functional categories for users, consider EMC Smarts’s security implementation. Document the implementation in the Deployment Build Guide.</td>
<td>“Users and security” on page 6-4</td>
</tr>
<tr>
<td></td>
<td>Define the Notification Lists in EMC Smarts user profiles.</td>
<td>The Notification List determines which notifications are sent from the Global Manager to the EMC Smarts client. Carefully define the Notification Lists, as they can affect Global Manager performance. Document the notification list provided for each user profile in the Deployment Build Guide.</td>
<td>“Designing notification lists” on page 6-5</td>
</tr>
<tr>
<td></td>
<td>Design console operations access.</td>
<td>Most operations that can be performed at the EMC Smarts clients can be individually enabled or disabled in the user profiles. Document the access provided for each user profile in the Deployment Build Guide.</td>
<td>“Designing consoles” on page 6-5</td>
</tr>
<tr>
<td></td>
<td>Design console layouts.</td>
<td>Specific console layouts can be saved and automatically provided to match user needs at the Global Console, Web Console, and Business Dashboard. Document the console layout used in each user profile in the Deployment Build Guide.</td>
<td>“Designing consoles” on page 6-5</td>
</tr>
<tr>
<td></td>
<td>Design client and server tools.</td>
<td>Define the necessary tools that users must access and the levels of programming skills required to create the tools. Document this information and tools provided by each user profile in the Deployment Build Guide.</td>
<td>“Planning for tools and tool deployment” on page 6-6</td>
</tr>
</tbody>
</table>
The EMC Smarts Business Impact Manager calculates the impact of infrastructure and application events on business services. This chapter describes the choices that must be made when designing business impact processing, and contains the following information:

- Designing business impact processing ................................................................. 7-2
- Importing information .......................................................................................... 7-4
- Business Impact Manager design checklist ......................................................... 7-5

**Note:** Complete configuration details are included in the *EMC Smarts Business Impact Manager User’s Guide.*
Deploying Business Impact Processing

Designing business impact processing

Business Impact Manager uses information from a Global Manager in conjunction with user-defined criteria to calculate the business impacts of infrastructure and application events.

To design business impact processing, you must consider at least these things:

- Business processes to model
- Topology of the business processes and the underlying infrastructure
- Impact (weight) caused by issues in the topology

Business processes

When designing a Business Impact Manager implementation, consider the company’s business processes. Try to answer the following questions:

- Which business processes exist?
- Which business processes depend on applications or network devices?

A business process represents functions and operations that support the internal business activities of an enterprise. In the manufacturing sector, for example, business processes include order processing, production planning, accounting, fulfillment, etc. Each of these may depend on different applications in order to operate as well as on network devices to pass information among and between applications and processes.

In a hypothetical situation, an order comes into a company and is processed. The processing involves entering the order into a Customer Relationship Management (CRM) application and simultaneously sending it to accounting for approval and fulfillment for shipping. Underlying accounting is a financials application and underlying fulfillment is a logistics application. Fulfillment begins preparing the order for shipping but cannot release the order until it receives approval from accounting. Once accounting approves the order, it notifies both fulfillment and ordering via a financials application that updates both the logistics and CRM applications. If a network device that supports the financials application exhibits problems, the fulfillment and CRM applications will not receive necessary updates, which has an impact on the business.

Try to map these dependencies in preparation for creating business topologies and weighting the impacts of problems on these processes. In the hypothetical situation, updating the logistics application, once accounting approves the order, may be a higher priority than updating the CRM application.

If the processes depend on applications, consider adding EMC Smarts Application Insight as part of the solution. See “Integrating with EMC Smarts Application Insight” on page 7-4 for more information about implementing a Business Impact Manager solution with EMC Smarts Application Insight.

Business topology

Once you have established the business processes, create a business topology to model them. The Business Impact Manager has special elements to describe business processes, including ServiceOffering, BusinessProcess, ServiceSubscriber, Customer, and others. The Business Impact Manager provides flexibility in classifying elements, but be consistent in your choices.
The names of these business elements or entities must be unique. The Global Manager assigns prefixes to the names of business elements to identify elements, but their display names do not include this prefix. When importing topology, remember to specify these names. When using a custom adapter to import topology, the element names must include the prefix.

The relationship between elements in the business topology is defined as part of an element’s definition. The next step in designing the business topology is to define relationships between business elements and other elements. As you do this, consider the following:

◆ How do infrastructure and other events affect business elements?
◆ What are the critical elements upon which the business elements rely?

In the case of an internet service provider (ISP), ServiceOffering represents the connections between a customer and the ISP. ServiceSubscriber represents a customer. You can make other choices. In this example, a ServiceOffering is a specific contract to provide a connection to a ServiceSubscriber.

The business topology gets linked to infrastructure elements through more definitions. The critical elements associated with a ServiceOffering are the customer routers. While the ISP edge routers are important, a ServiceOffering does not necessarily have to be associated with a particular router. When events affect customer routers, the ServiceOffering is directly affected. These routers are associated as members of the ServiceOffering.

Note: Since the ISP does not manage the customer routers, the ISP has only ICMP access to those routers. The ISP could choose to represent those routers as hosts.

Weights: Impacts of issues in the topology

Weight values are optionally set to indicate the magnitude of a problem but are not necessary to a Business Impact Manager installation. When a root-cause event occurs, the Business Impact Manager sums the weight of the affected elements for a total impact, which is displayed with the root-cause: the greater the impact number, the greater the problem. You can assign weights by class, instance name, and instance. Wildcards can be used when you assign weights by instance.

There is no particular method to use to assign weights. Weights measure the relative importance of aspects such as revenue, contractual requirements, reputation, cost, etc.

One strategy to follow when assigning weights is to develop weights from parent classes, through subclasses, down to particular instances. If there is any overlap, the instance weight is used before the class weight, which is used before the parent class weight.
Deploying Business Impact Processing

Importing information

There are two methods for importing Business Impact Manager information: import files and manually through a Global Console:

- For small Business Impact Manager configurations, such as demonstrations and test installations, manual configuration using the Topology Builder Console is a reasonable choice. Objects created through this console are stored only in the topology. You cannot modify elements not created with the Topology Builder or that are discovered by the underlying Domain Manager. Before you can use this console, you must set correct user privileges and permissions.

- For larger deployments, creating import files can ease the process. Import files provide an additional benefit in that they act as backup to the business topology. Do not use both methods to modify business topology. Elements added through one method are not modifiable by the other.

The structure of import files

When creating import files, consider the structure of the files. Especially when defining relationships, multiple files may be used to define one-to-many relationships. Business elements can be comprised of members and subscribers. Separate files may exist for these files or may exist for all of the different business elements.

The import files define business elements and service data, related infrastructure, and lists of related elements. The lists of related elements can be very useful when constructing relationships among large groups of elements, subscribers, or applications.

For more information on the syntax of the import files, see EMC Smarts Business Impact Manager User’s Guide.

Integrating with EMC Smarts Application Insight

Integration with EMC Smarts Application Insight allows you to monitor the health of your applications and see how changes in their status affects your business topology. The configuration of Business Impact Manager to Application Insight elements is beyond the scope of this guide. For more information, see the documentation provided with Application Insight.
Business Impact Manager design checklist

Each chapter in this guide includes a checklist. For ease of use, the checklists are also grouped in “Design and Deployment Checklists” on page A-1.

Table 7-1  Business Impact Manager design checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑</td>
<td>Define relevant business processes.</td>
<td>Determine the business processes to model. Record your choices in the Deployment Build Guide.</td>
<td>“Designing business impact processing” on page 7-2</td>
</tr>
<tr>
<td>❑</td>
<td>Create a business topology.</td>
<td>Create business elements to model the business processes. Define the expectations of the model and the events it should analyze. Document your topology in the Deployment Build Guide.</td>
<td>“Business topology” on page 7-2</td>
</tr>
<tr>
<td>❑</td>
<td>Assign weights to the elements of the topology.</td>
<td>This step is optional but allows you to assign a value to measure the impact of events that occur in the topology. The weights of impacted elements are summed in the root-cause event. Record your choices in the Deployment Build Guide.</td>
<td>“Weights: Impacts of issues in the topology” on page 7-3</td>
</tr>
<tr>
<td>❑</td>
<td>Choose a method for importing information.</td>
<td>If the topology is small, use the Topology Builder Console. For larger topologies, use one or more topology files. Record your choice in the Deployment Build Guide.</td>
<td>“Importing information” on page 7-4</td>
</tr>
</tbody>
</table>
This chapter describes important design considerations when installing EMC Smarts software. This chapter should be considered as a supplement, not a replacement, for the Installation Guides included with the EMC Smarts Service Assurance Management Suite software and for the EMC Smarts System Administration Guide. This chapter contains the following information:

- General installation/deployment guidelines ............................................................ 8-2
- Configuring the Java clients to use a proxy server ................................................... 8-5

Note: Consult the EMC Smarts Service Assurance Management Suite Installation Guide for detailed installation procedures and consult the EMC Smarts System Administration Guide for detailed configuration procedures.
Deploying Service Assurance

General installation/deployment guidelines

Many organizations have strict rules for deploying enterprise-level software which may include deployment of staging areas whenever possible. A staging area is a copy of the installation.

Never install a deployment during a normal production shift; instead, choose a period of low utilization for installation. If a test environment is not available, create a staging area (an environment that mirrors production) and make and test all changes in the staging area.

If possible, install the deployment in stages to reduce the size and complexity of each step in the overall process. Doing so makes debugging easier. Verify each stage of the deployment as described in the “Validating Your Deployment (Acceptance Testing)” on page 9-1.

EMC Smarts licensing

EMC Smarts licensing comes in two different forms: temporary and permanent. Temporary licensing is file-based, where each application uses a special license file. Permanent licensing uses a licensing server.

Information to collect for permanent licensing

For permanent licensing, EMC Smarts products rely on FLEXnet licensing software and a license file provided by EMC Smarts.

The FLEXnet software is installed with the EMC Smarts software, but a license file from EMC Corporation is also required. The license file must be installed using the install_license script as described in the EMC Smarts System Administration Guide. To generate the license, EMC Corporation needs the following information for the computer where the FLEXnet license server is running:

- The host ID
- The operating system
- The installation path to BASEDIR/smarts/bin on your Broker (or to the EMC Smarts installation from which you want to run the license server).

Send this information to the smartslicensing@emc.com e-mail address to ensure that an appropriate license is available for the deployment. Locating the license server

It is best to install the license server on the same host as the Broker. Both the license server and the Broker need to be able to communicate with various EMC Smarts applications.

Multiple license servers

When multiple license servers are used, each Domain Manager will use blocks of volume licenses from a specific license server. Therefore, the license blocks must be divided among multiple licenses; the appropriate license must be deployed to each license server. Then, Availability Managers that rely on a specific license server will have the appropriate volume licenses to support the systems they manage. If multiple license servers are used, ensure that EMC Corporation is aware of the configuration details.
EMC Smarts Service Assurance installation and configuration

As you install EMC Smarts applications, configure each application before installing the next application. EMC Corporation recommends the following installation order:

1. Broker (normally installed and configured when the first EMC Smarts components are installed)
2. A Global Console to use to verify the installation of other applications
3. Underlying domains (IP Availability Manager, IP Performance Manager, Network Protocol Manager, etc.) with associated adapters
4. Global Manager which includes Business Impact Manager, if licensed
5. Adapter Platform
6. EMC Smarts Adapters (that use Adapter Platform as a server)
7. Global Consoles for end users

To ease troubleshooting of the initial deployment, install limited segments of the deployment first. Always configure and validate a segment before installing the next segment.

By default, all EMC Smarts applications are installed as services and are started immediately after installation. During deployment, you should set the services to start manually until your installation, configuration, and validation are complete.

Setting environment variables

Setting inappropriate values for environment variables is a common cause of post-installation problems. Detailed descriptions of the EMC Smarts environment variables, including methods for setting them, are described in detail in the EMC Smarts System Administration Guide.

Configure security

Usernames and passwords

For initial validation, use the default administration user name and password (admin and changeme). Once you have validated your installation, change the default administration user name and password.

Security configuration files and a Secure Broker

A Secure Broker is a broker that requires authentication in order for EMC Smarts applications to use it. By default, the Broker is not secure. Universal access is provided to all EMC Smarts applications. By changing the password associated with the Broker, you configure a Secure Broker. EMC Smarts applications need to use the username and password to register with the Broker and also to connect to the Broker to determine the location of server applications.

Use and guard Your EMC Smarts secret phrase

EMC Smarts components are installed using a default secret phrase. This phrase is used to encrypt passwords used in authentication and to encrypt communications between EMC Smarts components.

EMC Corporation recommends that you take advantage of the added level of security provided through the secret phrase and its related security mechanisms. To do this, you must change the secret phrase using sm_rebond and make it consistent at all your EMC Smarts installation sites. Due to the sensitive and vital nature of this secret
Deploying Service Assurance

phrase, store and guard the phrase as you would do with the root passwords of the most sensitive servers in your network.

Under certain circumstances, the loss of the secret phrase can force extensive reconfigurations and require reinstallations of all EMC Smarts components.

Propagating the secret phrase

The recommended method to change the secret phrase for an EMC Smarts deployment is to run the sm_rebond utility in each installation area. Under certain circumstances, you can use one machine to create and encrypt the different configuration files as well as the imk.dat file.

It is best to do the propagation before the other applications are started. If you want to propagate the files and the server has started but there are no SNMP V3 passwords in use, replace the connection configuration files. If you are using SNMP V3 passwords, you will need to replace the connection configuration files, delete the existing repository files (*.rps), and restart the server.

The alternative to propagating all of the files is to propagate imk.dat then run for each file requiring security on each installation:

```
sm_edit --noedit <filename>
```

Deploy Business Impact Manager

Deploying the Business Impact Manager consists of the following tasks:

- Modify weights by changing weights.conf and applying the change using the ASL script, ICS_RemoteConfig.asl. Unless the weights are modified, each element will have the same value.
- Import business data. There are two methods for doing this: Create an import file and modify the appropriate section of the ics-default.xml file, or use the Topology Builder Console. Neither method can modify the results of the other.

Deploy user configurations

Deploying the user configurations consists of these tasks:

- Configure access to the software by adding user names and passwords to the security files (clientConnect.conf and serverConnect.conf) as described in the EMC Smarts System Administration Guide. These files define the security level for each user, including user capabilities, servers that can be accessed, and passwords.
- Configure users as described in the EMC Smarts Service Assurance Manager Configuration Guide:
  - Deploy and configure tools. Server tools must be copied to the server where Service Assurance is installed and client tools must be copied to all systems where Global Consoles are installed.
  - Create console configurations and then save them on the server where the Global Manager is installed. Create each console configuration by opening the Global Console and then arranging the layout and customizing preferences. Save the customized console.
  - Define customized Notification Lists.
  - Create user profiles that associate individual users with access to specific tools, consoles, and a Notification List.
Configuring the Java clients to use a proxy server

You can configure the Web Console, Business Dashboard, Dashboard viewlets, and Global Console to use a proxy server to communicate with EMC Smarts applications (for example, Availability Manager and Global Manager) that reside behind a firewall. Using a proxy server reduces the number of firewall ports that need to be opened to one firewall port.

For example, Figure 8-1 illustrates a typical deployment where a web server acts as the proxy server.

![Diagram of deployment with proxy server]

**Figure 8-1  Example of a deployment with a proxy server**

Before you configure these Java clients, ensure that the web server that will act as the proxy satisfies the requirement as described in “Requirement for proxy server” on page 8-6.

To configure the Java clients to use a proxy server, perform the following steps:

1. Your firewall administrator needs to open Port 80 on the firewall to enable communications between the client and a web server.

   Through a series of requests, the client communicates with a web server and that web server acts as the proxy to the EMC Smarts applications.

2. Use the sm_edit utility to add the Proxy properties described in Table 8-1 on page 8-6 to the appropriate properties file (where BASEDIR is /opt/InCharge7/SAM/smarts or C:\InCharge7\SAM\smarts): 

   - If you are using the Web Console (or Java Web Start), modify the webconsole.properties file in the BASEDIR/tomcat/webapps/webconsole directory.
If you are using the Business Dashboard and viewlets, modify the dashboard.properties file in the BASEDIR/tomcat/webapps/templates directory.

If you are using the Global Console, modify the BASEDIR/conf/console/properties.conf file on the machine where the Global Console is running.

The parameters, com.smarts.proxyAuthString and com.smarts.proxyAdditionalHeaders, are optional.

For com.smarts.proxyAuthString, the value would depend upon the type of authentication scheme the web server supports. For example, if it supports Basic Access Authentication Scheme, and if the Username is “User” and Password is “Password”, the value would be:

"Proxy-Authorization: basic VXNlcjpQYXNzd29yZAo=
"Then, string "VXNlcjpQYXNzd29yZAo=" would be the base64 encoding of, “User:Password”.

For com.smarts.proxyAdditionalHeaders, the value could be any valid HTTP request like this, for example:

▼ "GET http://www.example.com HTTP/1.1 \r\nHost: example.domain.com \r\n"▲

3. Modify the proxy connection settings in Internet Explorer. (This step is not applicable for the Global Console.)

- Open Internet Explorer and select Internet Options dialog from the Tools menu.
- In the Internet Options dialog, select the Connections tab.
- In the Connection tab, click the LAN Settings button.
- In the Local Area Network (LAN) Settings dialog, in the Proxy server section, select the checkbox for “Use a proxy server for your LAN”, and specify an IP address for the proxy server and port number. Click OK to save your changes.
- Click OK in the Internet Properties dialog.

Note: If you are using Java Web Start, it has a similar dialog in which you can specify the address for the proxy server and the port number.

### Requirement for proxy server

The connection time-out mechanism implemented in the EMC Smarts Service Assurance Management Suite makes use of a standard TCP feature known as urgent data or out-of-band data.

The HTTP proxy used with this code must pass the out-of-band data as is.
The RFCs that define the correct operation of HTTP proxies require that the proxies provide a transparent network connection. However, they do not explicitly mention support of out-of-band data.

Because of the large number of HTTP proxy implementations in use, EMC Corporation is not in a position to indicate which, if any, fail to correctly pass out-of-band data.

Please check if the proxy server you are considering passes out-of-band data. Contact EMC Global Services if the proxy server does not pass TCP urgent data.

If the proxy server fails to pass out-of-band data, connections will time out within about three minutes. The Global Manager or Domain Manager log will contain a message of the following form:

CI-E-EFLOWKEEPALIVESEND-Flow closing due to missed keepalive
This chapter describes how to ensure that your deployment operates as intended and contains the following information:

- Validation techniques ................................................................. 9-2
- Initial validation ........................................................................ 9-2
- Validating topology operations .................................................. 9-2
- Validating users and capabilities .............................................. 9-2
Validating Your Deployment (Acceptance Testing)

Validation techniques

When validating, begin by dividing the deployment into manageable, logical segments. Ensure each of the segments function properly and then perform end-to-end testing. Check data flow and then check the accuracy of the data itself. Validate as much as possible before discovering the topology so that you reduce complexity.

Initial validation

To start validation, ensure that the Broker has access to all the EMC Smarts Managers and that the EMC Smarts Manager processes are registered and running. Use brcontrol, as described in the EMC Smarts System Administration Guide, to list the processes registered with the Broker and their status.

Validating topology operations

After the topology of the network is discovered, it must be provided to the Global Manager from underlying domains or third-party software and then from the Global Manager to the Global Consoles. You must validate the topology before and after each exchange.

If the deployment includes an IP Availability Manager, ensure that you verify the topology at the Domain Manager as described in the EMC Smarts IP Management Suite Deployment Guide.

Validating trap processing

Use sm_snmp to generate traps to the SNMP Trap Adapter (Receiver) functioning as the trap exploder.

Ensure that you send traps that cause notifications from the underlying analysis servers as well as from the SAM Adapter configuration. Create a trap for each trap processing statement in the trap_mgr.conf file. If ASL scripting is included in the trap processing, ensure that the scripts function as intended.

Validating users and capabilities

To validate users and their capabilities, test each user profile. Create a temporary user for each of your user profiles. Log onto the Global Console as each user in turn and review the associated console capabilities including access to console operations, access to tools, configuration of the notification list, and layout of the console. Ensure that the capabilities match your expectations for each user profile.
This chapter describes methods for identifying performance problems in a Service Assurance deployment and the steps that you can take to correct these problems. This chapter contains the following information:

- Assessing performance ............................................................................................. 10-2
- Improving performance ........................................................................................... 10-11

Note: Regardless of the size of your deployment, always monitor its performance. If tuning is required, remember that tuning your deployment is an ongoing process that should be performed regularly.
Assessing performance

For the Global Manager, assess performance by checking the resources required by EMC Smarts processes against the operating system limits and by reviewing EMC Smarts performance metrics. The following methods:

- Monitoring Global Manager memory usage
- Monitoring Global Manager queues
- Monitoring EMC Smarts software with heartbeat notifications
- Monitoring topology synchronization performance
- Monitoring clients and threads
- Monitoring tool execution
- Monitoring escalation

Monitor Global Manager memory usage

Monitor memory usage by the Global Manager to ensure that it does not exceed the operating system’s memory limit and as a way to detect possible performance issues. Although monitoring memory usage should be part of a routine, these symptoms require immediate investigation:

- Fast memory growth after the Global Manager has reached a steady state, such as hundreds of megabytes of memory growth in a few hours. The steady state is typically reached sometime after startup: Be conservative and allow a few hours after startup before assuming that the Global Manager is in the steady state.
- Consistent memory growth over time, never reaching a plateau. This is only be relevant if the overall growth of the Global Manager process is also hundreds of megabytes of memory after reaching steady state.

Ensure that process size does not approach operating system limit

The memory limit is an operating system limit that indicates the maximum process size permitted in memory. This limit is seldom approached by the Global Manager process, but may become an issue for very large EMC Smarts topologies. The process size limits are shown in Table 10-1.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Memory limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>3.75 GB</td>
</tr>
<tr>
<td>HP-UX</td>
<td>2 GB</td>
</tr>
<tr>
<td>Linux</td>
<td>3.8 GB</td>
</tr>
<tr>
<td>Windows</td>
<td>2 GB</td>
</tr>
</tbody>
</table>

See the appropriate EMC Smarts Installation Guide for specific operating system version information. For more information on operating system limits, consult the operating system documentation.
To find the total size in memory for various EMC Smarts processes, use the following commands:

- For Linux or UNIX systems, use `ps -l -p proclist` where `proclist` is one or more IDs for the EMC Smarts processes. Review the total size of the processes in virtual memory.
- For Windows systems, open the Windows System Information tool and find the process size in the Software Environment, Running Tasks folder.

If an EMC Smarts process is approaching the memory limit, consult with EMC Smarts Professional Services for further evaluation.

**Establish and monitor a baseline for process memory size**

Under normal conditions with the Global Manager process memory size well within the operating system limit, monitor memory size to establish a baseline that can be used to detect performance issues early.

For UNIX systems, this can be automated by creating a script that periodically executes `ps -l -p proclist` and writes the output to a file. For Windows, similar functionality can be created using a batch file run by the Task Scheduler.

Investigating the values from the file helps to understand the memory growth pattern over time. Once the pattern is understood, it can be used to establish a baseline value for the memory usage of a running Global Manager.

The baseline value is then used to establish a memory usage threshold. Using a monitoring script, an alert can be generated if the memory used by the Global Manager ever exceeds the threshold.

Once the alert is received, investigate the queue growth before attempting to remedy the condition.

**Monitoring Global Manager queues**

Global Manager queue growth is often a cause of the Global Manager memory growth. Memory growth and queue growth are expected occasionally, due to large bursts of information processed. However, consistent growth of queues may indicate a problem.

**The dump queues command**

To monitor queues, EMC Smarts software provides a dump queues command that uses this syntax:

```
\> dmctl -s <server_name> exec dmdebug --queues
   -output=<file_name>
```

where:

- `<server_name>` is the name of the Global Manager.
- `<file_name>` is the name of the file where the output is written, such as `queues-010105-0100.out` (where 010105 is January 1, 2005, and 0100 is 1 AM). The file is written to the `smarts/local/logs` directory.
Monitoring the Performance of Your Deployment

Analyzing queue size

The queues output lists many queues. Monitor these queues closely:

- **SM_PropertyPoller**: This queue contains client requests for property subscriptions and data to be sent to clients as responses to property subscriptions. For example, in the Global Manager, notifications are sent to clients via property subscriptions. So, the property poller queue contains notifications to be sent to clients.

- **SubscriberFE**: This queue represents a connection the Global Manager server makes to another server, where the Global Manager server subscribes to information in another server. For example, there is a SubscriberFE queue for each underlying Domain Manager.

For each queue, the first line provides name of the queue and the number of workers. (Note that Subscriber Front Ends like this one never have any workers, since they are not used as normal server queues.)

The second line provides the current size, and an exact maximum size. Also included is the total number of entries “processed.” To be exact, this is the total number of entries that were pulled from the queue.

The next three rows provide averages. Each column reports values averaged over a different time interval: The last 3 minutes, 30 minutes, 300 minutes, and 3000 minutes. Each row reports a different value:

- **Size** is the queue size, that is, the average of what “Current size” reports for this moment
- **Flow** is the number of queue entries processed, that is, the average of what “Current processed entries” reports
- **Late** is the delay between when an entry in a timer queue was scheduled to run and when it actually ran. The Late row is always all 0’s for a server queue.

Each of the averages listed in the Size, Flow, and Late rows have two fields separated by a sign (+ or -):

- The first field is the average value of the variable over the appropriate period. The queue in Figure 10-1 has processed many entries -- almost 22,000 -- and once, even held 369 entries; but that was apparently an isolated peak some time in the past, since its average Size over all the reported intervals is 0: Most of the time, the queue is empty. On the other hand, the Flow value over the last 3 minutes is very close to the value for processed entries (21,843). If we look at this value averaged over longer and longer periods, we see that the longer the period, the smaller the
value. This is what we would expect if the rate at which elements are flowing through this queue is roughly constant. Always keep in mind that Size grows and shrinks, while Flow can only grow.

- The second field is the average rate of change in the first value, per second. In the example above, the Size is shrinking slowly: -0.0 indicates fewer than 0.01 entries per second. On the other hand, the Flow is increasing at a steady rate: between 0.05 and 0.06 entries per second (3.0 and 3.6 entries per minute) are flowing through this queue. Again, because Flow can only increase, the second field is always non-negative. Note that the rates are virtually the same across all time periods, which is consistent with the analysis in the previous paragraph that entries are flowing through at a slow, steady rate.

Guidelines for monitoring queues

Follow these guidelines:

- The queues output lists many queues. Queues that should be monitored more closely are SubscriberFE, and SM_PropertyPoller.

- Current size information is the most important to monitor. For most queues, this value is often 0. Some queues, such as ICS_ActionScheduler, almost always have non-zero values for current size. If the current size is not zero and grows over several successive dump queues commands, it should be further analyzed.

Establish and monitor a baseline for queue size

Under normal conditions, monitor queue size to establish a baseline that can be used to detect performance issues early.

To set up automatic monitoring of queues, a script may be written to parse the output of the dump queues. The script could specifically parse the current size for each queue. For example, if the current size exceeds a specified threshold, then alert someone to investigate this further. Some queues would need to be exempt from the threshold, such as ICS_ActionScheduler.

A possible threshold for queues would be 10,000. However, this setting would depend on your specific needs. It would also be possible to set the threshold lower. If you set a lower threshold, you should do more monitoring to determine whether or not there is a consistent queue growth.

If queue growth happens consistently over time, further investigation is recommended.

Monitoring with heartbeat notifications

To monitor the throughput of notifications by a Global Manager, you can implement a mechanism to create heartbeat notifications. These notifications are generated in Domain Managers or Adapter Platforms on a periodic basis. The notifications are propagated from the lower level domains to the Global Manager or through multiple levels of Global Manager.

A custom adapter listens for these notifications at the Global Manager. The custom adapter monitors the rate of receipt of the notifications from each of the underlying domains.

If a notification is not received within a predetermined period after it is generated, appropriate personnel are alerted automatically for further investigation. This investigation would entail determining if there is a consistent delay from either of the following:
Monitoring the Performance of Your Deployment

- One particular EMC Smarts domain: If the delay is from one domain, analyze the domain. Consult the appropriate deployment guide for the domain.
- All EMC Smarts domains: If the delay is from all domains, analyze the Global Manager. Analyze the Global Manager memory usage, queues, and topology synchronizations as described in this chapter.

The heartbeat notifications must be filtered so that they are not displayed in the Global Consoles. This would add an unnecessary burden to the Global Console users. Configure the notifications lists to eliminate the heartbeat notifications.

EMC Smarts Global Services or Professional Services can aid in deploying heartbeat notifications for monitoring.

Monitoring topology synchronization

Topology synchronization information is written to the Global Manager log file. This information indicates when the Global Manager starts and ends a topology synchronization with an underlying domain. Topology synchronization is one of the more resource intensive aspects of processing in the Global Manager. Therefore, it is important when analyzing Global Manager performance to determine the following information about topology synchronizations:

- How many topology synchronizations occur over a period?
- How frequently are individual domains synchronizing topology?
- How long did each topology synchronization take?

The log file contains a significant amount of information. To extract only the topology synchronization information, use `grep`. The gnu version of `grep` provides an option to return lines above and below the matching line, which is very helpful in this case.

For example, using `/opt/gnu/bin/grep -C1 "Topology Synch"` will return a similar line to the sample in the Figure 10-2. Note that the “-C1” option returns one line above and one line below the matched line.

```
[06-Jul-2004 13:57:27+522ms EST]
ICS-W-ics-event-processing.asl: 'IC-AM1' - Topology Synchronization has started
--
[06-Jul-2004 14:01:46+737ms EST]
ICS-W-ics-topology-sync.asl: IC-AM1' - Topology Synchronization has ended
--
[06-Jul-2004 14:13:46+172ms EST]
ICS-W-ics-topology-sync.asl: 'IC-AM2' - Topology Synchronization has ended
--
[06-Jul-2004 14:42:10+151ms EST]
ICS-W-ics-event-processing.asl: 'IC-AM1' - Topology Synchronization has ended
--
[06-Jul-2004 14:42:57+528ms EST]
ICS-W-ics-topology-sync.asl: 'IC-AM1' - Topology Synchronization has ended
```

Figure 10-2 Global Manager Topology Synchronization Information Example

Figure 10-2 shows two topology synchronizations from IC-AM1, an Availability Manager, during the log file monitoring period:

- Started on July 6 at 13:57 and then ended at 14:01.
- started on July 6 at 14:42 and then ended at 14:42.
Another topology synchronization was in progress from IC-AM2 which ended at 14:13. The start time is not included in the log file.

A slow topology synchronization may not be an issue. Since topology synchronization occurs in the background, its duration does not necessarily impact general processing of the Global Manager. If there is a long latency in the connection from Global Manager to the underlying domain that it is synchronizing with, the topology synchronization may take longer and yet not affect Global Manager. Also, topology synchronization will take longer for larger topologies than smaller topologies.

However, it may be a symptom that the Global Manager is overloaded and is trying to process more than it can handle. If the Global Manager is overloaded, you may see long topology synchronization times, slow performance when viewing information in the console, and possibly even delays in processing notifications.

Since topology synchronization is one of the Global Manager processing tasks, improving control of topology synchronization may be a way to improve performance.

For example, it is possible to make small topology changes on an underlying domain at a high frequency or larger topology changes at a low frequency on an underlying domain. Global Manager performance will be better if a low frequency of larger topology changes are made. The frequency of topology changes can be controlled partially in underlying domains by adjusting the periodic and full discovery intervals. Also, an EMC Smarts administrator can initiate discoveries. The frequency of these on-demand discoveries may affect Global Manager performance; minimize them when possible.

Another topology synchronization consideration is the number of underlying domains communicating with Global Manager and the concurrency of the topology synchronization of these. If there are a large number of domains, there is an increased likelihood of concurrent topology synchronizations of underlying domains. Since topology synchronization is one of the more intensive processing done by Global Manager, having multiple topology synchronizations happen concurrently may cause console performance and notification throughput to slow down.

---

**Periodic dump threads and dump clients**

EMC Smarts provides a number of different monitoring utilities, including:

- Listing thread information from a running EMC Smarts server
- Listing attached clients for a running EMC Smarts server

**Listing thread information**

These can be executed using the command:

```
$dmctl -s <server_name> exec dmdebug dumpThreads -output=<file_name>
```

The output of threads is shown in Figure 10-3 on page 10-8.
Monitoring the Performance of Your Deployment

Figure 10-3 Global Manager threads information example

Figure 10-3 lists running threads in the server. This gives an idea of the type of processing done in the server. This is often used in conjunction with a pstack output. This information is not typically monitored, but often used in investigating issues.

Listing client information

This command displays a list of all clients attached to an EMC Smarts server, including adapters.

```
  dmcctl -s <server_name> exec dmdebug dumpClients -output=<file_name>
```

Figure 10-4 shows an example of dump clients output.

Remote Clients [21-Oct-2004 10:05:05 GMT] -
Id User Privs Host PID Since Description
--------------------------------------------------
5 Administrator PING+READNETVISTAM42-SAM unknown 10-Oct-2004 11:08:21 GMT IC Console

Input:
Socket 101, mode Read; 0/2048 bytes, lasterr 0, no timeout
Desktop1:2180 -> 192.6.17.52:3073
00000000 00000020 526F7574 65720000 000B5243 4C4F4E35 30303938 30000000
Output:
Socket 101, mode Write; 0/2048 bytes, lasterr 0, no timeout
Desktop1:2180 -> 192.6.17.52:3073
28284950 20416464 72657374 32057269 77697468 64697370 6173204E 616D6573

10 root ALL server1 1061 18-Oct-2004 11:08:21 GMT ASL
Input:
Socket 151, mode Read; 0/2048 bytes, lasterr 0, no timeout
Server1:2180 -> server2:63325
00000048 00000014 49344535 4F486F77 66696E64 6966656C 652E616E
Output:
Socket 151, mode Write; 0/2048 bytes, lasterr 0, no timeout
Server1:2180 -> server2:63325
28284950 20416464 72657374 32057269 77697468 64697370 6173204E 616D6573

Figure 10-4 Global Manager client information example

The example in Figure 10-4 shows one console client, “IC Console”, and one ASL client, “ASL”. The output gives the time the connection was initiated, the privileges associated with the connection, and the host the client runs on.
Monitoring tools

Tools are programs that can be invoked automatically by the Global Manager or through the Global Console by an operator. The tools should be monitored using the following EMC Smarts utility to ensure that they do not adversely affect performance:

```
dmctl -s <server_name> invoke ICS_ActionManager::ICS-ActionManager dumpStatistics <string> filename
```

Summary:
- number_of_sync_actions_executed: 7
- max_execution_time: 30.6950 secs
- avg_execution_time: 9.3593 secs

number_of_successfull_sync_actions: 5
number_of_timeout_sync_actions: 2
number_of_failed_sync_actions: 0

Details:
- Action ID: ICS-ServerProgramAction-Sample - Close Trouble Ticket
  - No of times invoked: 1
  - Maximum Execution time: 1.3720 secs
  - Average Execution time: 1.3720 secs
  - No of Successful Execution: 1
  - No of Timeouts: 0
  - No of Failures: 0

- Action ID: ICS-AutoProgramAction-Set UserDefined1
  - No of times invoked: 1
  - Maximum Execution time: 0.5410 secs
  - Average Execution time: 0.5410 secs
  - No of Successful Execution: 1
  - No of Timeouts: 0
  - No of Failures: 0

- Action ID: ICS-ServerProgramAction-Sample - Open Trouble Ticket
  - No of times invoked: 1
  - Maximum Execution time: 1.8720 secs
  - Average Execution time: 1.8720 secs
  - No of Successful Execution: 1
  - No of Timeouts: 0
  - No of Failures: 0

- Action ID: ICS-AutoProgramAction-Esc-Paging
  - No of times invoked: 4
  - Maximum Execution time: 30.6950 secs
  - Average Execution time: 15.4325 secs
  - No of Successful Execution: 2
  - No of Timeouts: 2
  - No of Failures: 0

Figure 10-5 Output of the Dumpstatistics option for tools

The tools monitored by the utility include all synchronous tools (server and automatic). Asynchronous tools (client tools), which are client tools invoked by users from the Global Console, are not monitored using this utility.

Monitoring escalation

EMC Smarts software provides a utility that can monitor escalation, including statistics for each escalation level in every escalation path configured in the Global Manager. The syntax is as follows:

```
dmctl -s <server_name> invoke ICS_AutoActionManager::ICS-AutoActionManager dumpStatistics <string>fileName
```
Monitoring the Performance of Your Deployment

Figure 10-6 shows the sample output for the Dumpstatistics option for escalation. The following values are included as a total for all escalation paths and for each level in each path:

- Number of executed jobs. A job is a scheduled notification that matched a policy-path and that repeats for each level in that path. The number of executed jobs is indicated for all levels in all paths (overall) and for each level.

- Total, maximum, and average execution times. Execution time indicates how long the tool actions defined for a job took in seconds. If the maximum execution time at a level far exceeds the average, it may indicate an issue for a particular tool.

- Total, maximum, and average queue delays for all the escalation paths is also displayed. These delays are not related to execution time. Delay is difference between when a job was scheduled to execute and when the job was actually executed. A positive value for the delay indicates that the system is not keeping up with scheduled escalation. Delay may be caused by the overall load on the server, number of notifications, policies, paths, or levels. When a burst of notifications make it into a path, all jobs are scheduled to execute at the same time in a future time, so delay may increase due to these bursts.

To improve escalation performance, see “Increase worker threads for escalation” on page 10-12.

<table>
<thead>
<tr>
<th>Time stamp: [20-May-2003 05:49:05 PM EDT]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalation Statistics (All times are in seconds)</td>
</tr>
<tr>
<td>OVERALL:</td>
</tr>
<tr>
<td>number_of_executed_jobs : 122</td>
</tr>
<tr>
<td>total_execution_time     : 10.0430</td>
</tr>
<tr>
<td>max_execution_time       : 0.3024</td>
</tr>
<tr>
<td>avg_execution_time       : 0.0823</td>
</tr>
<tr>
<td>total_queue_delay        : 5.0068</td>
</tr>
<tr>
<td>max_queue_delay          : 0.2419</td>
</tr>
<tr>
<td>avg_queue_delay          : 0.0410</td>
</tr>
<tr>
<td>LEVEL Policy1-Path1-0:</td>
</tr>
<tr>
<td>number_of_executed_jobs : 4</td>
</tr>
<tr>
<td>total_execution_time     : 0.8123</td>
</tr>
<tr>
<td>max_execution_time       : 0.2856</td>
</tr>
<tr>
<td>avg_execution_time       : 0.2031</td>
</tr>
<tr>
<td>LEVEL Policy1-Path1-1:</td>
</tr>
<tr>
<td>number_of_executed_jobs : 0</td>
</tr>
<tr>
<td>total_execution_time     : 0.0000</td>
</tr>
<tr>
<td>max_execution_time       : 0.0000</td>
</tr>
<tr>
<td>avg_execution_time       : 0.0000</td>
</tr>
<tr>
<td>LEVEL Policy1-Path1-2:</td>
</tr>
<tr>
<td>number_of_executed_jobs : 0</td>
</tr>
<tr>
<td>total_execution_time     : 0.0000</td>
</tr>
<tr>
<td>max_execution_time       : 0.0000</td>
</tr>
<tr>
<td>avg_execution_time       : 0.0000</td>
</tr>
<tr>
<td>LEVEL Policy2-Path2-0:</td>
</tr>
<tr>
<td>number_of_executed_jobs : 118</td>
</tr>
<tr>
<td>total_execution_time     : 9.2307</td>
</tr>
<tr>
<td>max_execution_time       : 0.3024</td>
</tr>
<tr>
<td>avg_execution_time       : 0.0782</td>
</tr>
</tbody>
</table>

Figure 10-6 Output of the Dumpstatistics option for escalation
Improving performance

If the performance metrics indicate a performance degradation, try the following tactics to improve performance:

- Refine notification lists for users
- Reassess the topology synchronization configuration
- Refine sets of trap, syslog notifications sent to SAM
- Increase worker threads used for escalation
- Redesign your deployment to deploy additional Global Managers in a hierarchical Service Assurance configuration

Refine notification lists for users

A Notification List determines the events that are forwarded to a user. Essentially, the list filters the notifications that are sent from the Global Manager and can be assigned to one or more users.

In large Service Assurance deployments, significant numbers of notifications are active at any given time. Displaying all of these notifications to all users may adversely affect the performance of the system. Instead, create notification lists that are focused on providing groups of users with only the notifications that are specifically useful to them. This approach will improve performance and may also simplify users’ tasks by allowing them to focusing their efforts on appropriate notifications.

Reassess configuration of topology synchronization

As described in “Designing for Topology Operations” on page 4-1, the frequency of topology changes can be controlled partially in underlying domains by adjusting the periodic and full discovery intervals. If the pace of change in your network and application infrastructure can be supported with longer discovery intervals, increasing the interval may also improve Global Manager performance.

Because discovery can also initiated manually, another method to improve performance may be to reduce the frequency of manual discoveries. Reassess access to ad hoc discovery and remove it from the user profiles of administrators who do absolutely not require it. For administrators who retain access to manual discovery, educate them on the effect of initiating an unscheduled discovery.

Refine set of trap and syslog notifications sent to Global Manager

The notifications that result from analysis by EMC Smarts Managers typically contribute very little to the notification load on Global Manager. During analysis, EMC Smarts Managers reduce the load by analyzing numerous traps and polling results to produce a notification for each root cause rather than the symptoms.

Do not forward traps to the Global Manager when they are already sent to a Domain Manager for analysis. Use the first match in trap forwarding configuration file, if possible. If you have not implemented batching at the EMC Smarts SNMP Trap Adapter, do so.

See “Designing trap processing” on page 5-4 for more information.
Monitoring the Performance of Your Deployment

Increase worker threads for escalation

If the performance metrics indicate a performance degradation in Escalation, add worker threads to improve performance. Increasing threads to 10 worker threads is acceptable, but keep in mind that more threads may require additional or more capable CPUs. Be conservative when increasing threads: This action may reduce the overall resources that are available and affect performance. Increase the value in the ics-default.xml file. Then reconfigure the Global Manager, as described in the EMC Smarts Service Assurance Manager Configuration Guide.

Note that once increased, the number of worker threads cannot be reduced unless the server is restarted.

Upgrade server hardware

Improve the capabilities of the equipment where the EMC Smarts process is installed: Use a faster CPU or reinstall EMC Smarts software on more capable equipment. Before resorting to this hardware upgrade, consider the previous options.

Redesign the Service Assurance deployment

If, after attempting the other methods to improve performance, there are still issues, then determine if your actual deployment has exceeded the original deployment design.

If this is the case, you may have to deploy additional Global Managers in a hierarchical Service Assurance configuration. To start redesigning a deployment, return to “Designing the Service Assurance Deployment” on page 3-1.
This Appendix gather the checklists that are included throughout this guide into a single, easily accessible location. The checklists included in this chapter are:

- Before you begin checklist ................................................................. A-2
- Basic information checklist ............................................................... A-3
- EMC Smarts design checklist ............................................................. A-4
- Designing topology operations checklist ............................................. A-5
- Planning for notifications checklist .................................................... A-6
- EMC Smarts client and user design checklist ...................................... A-7
- Business Impact Manager design checklist ....................................... A-8
### Before you begin checklist

#### Table A-1 Before you begin checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
</table>
| ❑        | Possess an understanding of the EMC Smarts architecture and capabilities.   | At a minimum, you must understand the concepts and EMC Smarts architecture described in the following documents:  
  • EMC Smarts Service Assurance Manager Introduction  
  • EMC Smarts Service Assurance Manager Configuration Guide  
  • EMC Smarts Service Assurance Manager Adapter Platform User's Guide  
  • EMC Smarts System Administration Guide  
  • EMC Smarts IP Management Suite Installation Guide that accompanied your software product suite  
  • EMC Smarts user's guides related to the underlying EMC Smarts domains in your deployment  
To improve your understanding, attend EMC Smarts training courses offered by EMC® Education Services and Development. Typically, deployment requires the knowledge equivalent to what is provided in the training courses on:  
  • EMC Smarts Global Manager  
  • EMC Smarts Service Assurance Manager Adapter Platform  
  • Any underlying EMC Smarts domain that will be part of your deployment. |
| ❑        | Obtain contact information for the deployment team.                         | The contact list should include titles, responsibilities, and contact methods for all team members.                                                                                                        |
| ❑        | Get nondisclosure requirements and negotiate an agreement.                  | Be aware of the requirements of the non-disclosure agreements that are in place for the EMC Smarts deployment.                                                                                  |
| ❑        | Develop schedules and set milestones for early deliverable.                 | Scheduling a software deployment varies based on the size and scope of the deployment and the organization's requirements. Typical milestones might include:  
  • Initial project meeting to define the deployment scope  
  • Purchase of EMC Smarts software  
  • Project development begins  
  • Installation in test environment complete  
  • Testing complete  
  • Installation in production environment complete  
  • EMC Smarts goes live  
Additional information on scheduling is beyond the scope of this guide. |
### Basic information checklist

#### Table A-2 Basic Service Assurance information checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Describe the organization's requirements and expectations.</td>
<td>Document these requirements and expectations in the Deployment Build Guide.</td>
<td>“Determine the organization’s requirements” on page 2-3</td>
</tr>
</tbody>
</table>
| 0        | Obtain network diagrams.                                            | Ensure that the diagrams include the locations of the following:  
• The physical geography of the network  
• Locations of Network Operations Centers (NOC’s)  
• Lower speed WAN links such as T1 links  
• Numbers of devices  
If possible, include the network diagram in the Deployment Build Guide. | “Obtain network and application information” on page 2-3                                   |
| 0        | Describe the organization's network and application priorities.     | Document these priorities in the Deployment Build Guide.                                                                                                                                                     | “Determine network and application priorities” on page 2-5                                |
| 0        | Determine the number of managed devices and applications in the environment. | Document all quantities in the Deployment Build Guide.                                                                                                                                                       | “Determine how many devices and applications will be managed” on page 2-6                 |
| 0        | Estimate potential growth in quantity of managed devices.           | The EMC Smarts deployment must support potential network growth. Estimate the growth over a specific time period. Document the calculations in the Deployment Build Guide.                              | “Determine how many devices and applications will be managed” on page 2-6                 |
| 0        | Get the organization’s testing/acceptance requirements.             | Your design may be required to meet test and acceptance requirements. Obtain any specifications that cover integration testing, user acceptance testing, and operational acceptance testing. You may be required to write an installation or deployment report that follows an organization’s particular standards. | “Determine requirements for installing software” on page 2-8                              |
| 0        | Describe the organization’s requirements for installing new software. | Document these requirements and how the design meets them in the Deployment Build Guide.                                                                                                                     | “Determine requirements for installing software” on page 2-8                              |
| 0        | List the products that currently monitor the network.               | Document the products (including version) in deployment Build Guide.                                                                                                                                       | “Define requirements for integrating existing software with EMC Smarts” on page 2-8      |
| 0        | Describe the network security.                                      | Describe security features that will affect the deployment. Document the security features in the Deployment Build Guide.                                                                                   | “Gather network security information” on page 2-9                                         |
| 0        | List any other network requirements or features that may affect the deployment. | Document the features in the Deployment Build Guide.                                                                                                                                                      | “What other network features affect EMC Smarts?” on page 2-10                             |
## EMC Smarts design checklist

### Table A-3 Initial design checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>Determine the configuration of the Service Assurance Deployment.</td>
<td>Determine Service Assurance configuration, including the numbers of Global Managers and how they are organized in the EMC Smarts deployment.</td>
<td>“Determine the Service Assurance configuration” on page 3-2</td>
</tr>
<tr>
<td>o</td>
<td>Determine the hardware required to support the Service Assurance Deployment.</td>
<td>For each Global Manager in the Service Assurance configuration, determine the type of equipment required to support it.</td>
<td>“Hardware for Service Assurance platform equipment tiers” on page 3-7</td>
</tr>
<tr>
<td>o</td>
<td>Determine the location of the EMC Smarts Broker</td>
<td>Choose a location for the EMC Smarts Broker that will support the EMC Smarts deployment.</td>
<td>“Locating EMC Smarts Brokers” on page 3-9</td>
</tr>
<tr>
<td>o</td>
<td>Determine the location of the License Server</td>
<td>Choose a location for the EMC Smarts License Server that will support the EMC Smarts deployment.</td>
<td>“Locating license servers” on page 3-9</td>
</tr>
<tr>
<td>o</td>
<td>Determine the location of the EMC Smarts Global Manager(s)</td>
<td>Choose locations for the one or more EMC Smarts Global Manager(s) that will support the EMC Smarts deployment.</td>
<td>“Locating the Global Managers in the network” on page 3-11</td>
</tr>
<tr>
<td>o</td>
<td>Determine if Service Assurance Manager must be configured with failover.</td>
<td>Determine if a high availability configuration is required.</td>
<td>“Considering failover (high availability) configurations” on page 3-13</td>
</tr>
<tr>
<td>o</td>
<td>Determine if acceptance test are required.</td>
<td>Acceptance tests may be required for different portions of EMC Smarts functionality. Be aware of the requirements and develop acceptance criteria.</td>
<td>“Designing acceptance tests” on page 3-14</td>
</tr>
</tbody>
</table>
### Designing topology operations checklist

**Table A-4  Designing topology operations checklist**

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Review topology synchronization issues.</td>
<td>Ensure that you understand how topology synchronization affects Global Manager performance.</td>
<td>“Understanding topology synchronization” on page 4-2</td>
</tr>
<tr>
<td>0</td>
<td>Plan topology synchronizations.</td>
<td>To optimize Global Manager performance, it is best to reduce the number of topology synchronizations where possible.</td>
<td>“Planning for topology synchronization” on page 4-3</td>
</tr>
<tr>
<td>0</td>
<td>Plan topology groups.</td>
<td>Topology grouping is a visual tool that doe not affect Global Manager performance. Groups help organize topology elements.</td>
<td>“Designing topology groupings” on page 4-4</td>
</tr>
</tbody>
</table>
### Planning for notifications checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Determine which notification are important for EMC Smarts operators.</td>
<td>Ensure only the notifications that are useful to Global Console operators reach the Global Manager.</td>
<td>“Overview of notification processing” on page 5-2</td>
</tr>
<tr>
<td></td>
<td>Configure Notification Lists.</td>
<td>Notification lists are the mechanism that clients use to subscribe to and receive notifications from a Global Manager.</td>
<td>“Configuring notifications for clients” on page 5-3</td>
</tr>
<tr>
<td></td>
<td>Design Trap Processing.</td>
<td>Any EMC Smarts deployment should include a plan to handle trap processing.</td>
<td>“Recommended trap processing design” on page 5-4</td>
</tr>
</tbody>
</table>
# EMC Smarts client and user design checklist

## Table A-6  EMC Smarts client and user design checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Define functional groups for users.</td>
<td>List the broad functional groups that users will belong to and then define</td>
<td>“Who are the Global Manager users?” on page 6-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the needs and duties of each group. Add this information to the Deployment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Choose appropriate EMC Smarts clients for users.</td>
<td>EMC Smarts consoles have different capabilities. For each type of user</td>
<td>“Choose a console for types of users” on page 6-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and their equipment, you must determine which console is most appropriate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document your choices in the Deployment Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Define how you will implement security for</td>
<td>When defining the functional categories for users, consider EMC Smarts’s</td>
<td>“Users and security” on page 6-4</td>
</tr>
<tr>
<td></td>
<td>user groups.</td>
<td>security implementation. Document the implementation in the Deployment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Define the notification lists in EMC Smarts</td>
<td>The Notification List determines which notifications are sent from the</td>
<td>“Designing notification lists” on page 6-5</td>
</tr>
<tr>
<td></td>
<td>user profiles.</td>
<td>Global Manager to the EMC Smarts client. Carefully define the notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>lists as they can affect Global Manager performance. Document the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>notification list provided for each user profile in the Deployment Build</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Design console operations access.</td>
<td>Most operations that can be performed at the EMC Smarts clients can be</td>
<td>“Designing consoles” on page 6-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>individually enabled or disabled in the user profiles. Document the access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>provided for each user profile in the Deployment Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Design console layouts.</td>
<td>Specific console layouts can be saved and then automatically provided to</td>
<td>“Designing consoles” on page 6-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>match user needs at the Global Console, Web Console, and Business</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dashboard. Document the console layout used in each user profile in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deployment Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Design client and server tools.</td>
<td>Define the necessary tools that users must access and the levels of</td>
<td>“Planning for tools and tool deployment” on page 6-6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>programming skills required to create the tools. Document this information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and tools provided by each user profile in the Deployment Build Guide.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Define functional groups for users.</td>
<td>List the broad functional groups that users will belong to and then define</td>
<td>“Who are the Global Manager users?” on page 6-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the needs and duties of each group. Add this information to the Deployment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Build Guide.</td>
<td></td>
</tr>
</tbody>
</table>
## Business Impact Manager design checklist

<table>
<thead>
<tr>
<th>Complete</th>
<th>Task</th>
<th>Description</th>
<th>Related documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>Define relevant business processes.</td>
<td>Determine the business processes to model.</td>
<td>“Designing business impact processing” on page 7-2</td>
</tr>
<tr>
<td>o</td>
<td>Create a business topology.</td>
<td>Create business elements to model the business processes. Define the expectations of the model and the events it should analyze.</td>
<td>“Business topology” on page 7-2</td>
</tr>
<tr>
<td>o</td>
<td>Assign weights to the elements of the topology.</td>
<td>This step is optional but allows you to assign a value to measure the impact of events that occur in the topology. The weights of impacted elements are summed in the root-cause event.</td>
<td>“Weights: Impacts of issues in the topology” on page 7-3</td>
</tr>
<tr>
<td>o</td>
<td>Choose a method for importing information.</td>
<td>If the topology is small, use the Topology Builder Console. For larger topologies, use one or more topology files.</td>
<td>“Importing information” on page 7-4</td>
</tr>
</tbody>
</table>
Index

A
Adapter
  Syslog 1-2
Adapter Platform 5-2, 8-3
Adapters 2-8
  Concord eHealth 2-8
  InfoVista 2-8
Aggregation Layer 3-2
Architecture
  general 1-2
Architecture Solution Diagram 3-8
ASL 5-7
ASL Scripts 5-6
Authentication 8-3, 8-6

B
Basic Hierarchical Configuration 3-3
Batching Traps 5-5, 5-7
Before You Begin Checklist 1-7, A-2
BIM 7-1
brcontrol 9-2
Broker 3-9
  Default Port 3-9, 3-12
  Secure 8-3
Build Guide 1-5, 2-2, 3-8
Business Dashboard 1-2, 6-3
Business Impact Manager 1-2, 7-1

C
Checklists
  Before You Begin 1-7, A-2
  Discovery Design 5-9, A-6
clientConnect.conf 6-4
Clients 2-6, 3-2, 6-3
Concord eHealth 2-8
Configurations 3-3 to 3-6
  Basic Hierarchical 3-3, 3-11
  Hierarchical Aggregation 3-4, 3-11, 4-3
  Hierarchical Mesh 3-6, 3-11, 4-3
  Hierarchical Presentation 3-5
  Password 6-4
  Security 8-3

Service Assurance 8-3
Standard 3-3
Consoles
  Clients 6-3
  Defining 6-5
  Designing 6-5
  Layouts 6-5
  Restricting operations 6-5
  Web 3-5

D
dashboard.properties 8-6
Deploy
  Global Manager 3-8
Deploy Domain Managers 3-8
Deployment
  Build Guide 1-5, 2-2, 3-8
  Design description 1-4
  Installation and configuration description 1-5
  Phases 1-4
  Process 1-4
  Tools 6-6
  Tuning description 1-6
  Validation description 1-6
Deployment Process 1-4
  Designing 1-4
  Installing and Configuring 1-5
  Validating 1-6
Designing
  Consoles 6-5
Discovery Design Checklists 5-9, A-6
DNS 5-7
Domain Manager 1-2
  Deploy 3-8
Domains
  Underlying 3-2
Dump Queues 10-3

E
Environment Variables 8-3
Index

F
Failover capabilities 2-10
Filtering Traps 5-7
Firewalls 2-9, 8-5
FLEXnet 3-9

G
Global Console 6-3
Function 1-2
Global Console Users
Categories 6-2
Security 6-4
Global Manager 1-2
Deploy 3-8

H
Hardware 3-7
Heartbeat Notifications 10-5
Hierarchical Aggregation Configuration 3-4, 4-3
Hierarchical configuration 3-3
Hierarchical Mesh Configuration 3-6, 4-3
Hierarchical Presentation Configuration 3-5
Hook Script 5-7
Host Name Lookup 5-7
HTTP 8-6

I
ICS ActionScheduler 10-5
InfoVista 2-8
Installation
Service Assurance 8-3
Integrating Existing Software 2-8

J
Java Applets 6-3

L
Latency 2-10, 3-5, 3-11, 10-7
Layers
Aggregation 3-2
Presentation 3-2
Layouts 6-5
License Manager
Port 3-12
Licensing
Configurations 3-9
Generating a license 8-2
Multiple License Servers 3-9
Permanent 8-2

M
Memory 10-2 to 10-3
Process size limit 10-2
MIBs 3-12
Monitoring Utilities 10-7

N
Network
Firewall 2-9
Security 2-9
Size 3-2
Network Management 2-10
NOC 2-3
Notifications
Heartbeat 10-5
Lists 5-3, 6-5, 10-11
Processing 5-2 to 5-3
Syslog 10-11
Traps 10-11

O
Out of Band 2-10, 8-6

P
Password Configuration 6-4, 8-3
Performance
Guidelines 10-2
Improving 10-11
Trap Processing 5-7 to 5-8
Ports 3-12
Broker 3-9, 3-12
License Manager 3-12
Presentation Layer 3-2
Process Size Memory Limit 10-2
Profiles 6-5
properties.conf 10-2
Proxy Server 3-12, 8-5

Q
Queue
Growth 10-3
Size 10-4

R
Requests for Proposal (RFPs) 2-3

S
SAM Adapter Platform
Function 1-2
Secret Phrase 8-3
Secure Broker 8-3
Security 2-9, 3-12, 6-4
clientConnect.conf 6-4
Configuration 8-3
Global Console Users 6-4
serverConnect.conf 6-4
Users 6-4, 8-3
Server Tools 2-8
serverConnect.conf 6-4
Service Assurance Adapters 1-2
Service Assurance Configuration 8-3
Service Assurance Installation 8-3
Service Assurance Manager 1-2
Global Console function 1-2
SM_PropertyPoller 10-4, 10-5
sm_snmp 9-2
SNMP Trap Adapter 3-12, 5-4
Software
Integrating Third-party 2-8
Solution Architecture Diagram 1-5, 2-2, 3-11
Standard Configuration 3-3
SubscriberFE 10-4, 10-5
Syslog
Notifications 10-11
Syslog Adapter 3-12
Function 1-2

TCP 2-9, 3-12
Tool Deployment 6-6
Topology 5-7
Browser Views 6-6
Grouping 4-4
Synchronization 3-4, 4-2 to 4-3, 10-6, 10-11
Validating 9-2
Trap
Explooder 5-4
Notifications 10-11
Trap Processing
Adding New Topology 5-7
ASL scripts 5-4, 5-6
Batching 5-5
Filtering 5-7
Host Name Lookup 5-7
Notifications 5-6
Performance 5-7
Ports 5-6
Recommended design 5-4
Validation 9-2
trap_mgr.conf 5-7, 9-2
trapd.conf 5-6

UDP 2-9, 3-12
Underlying Domains 3-2
User Profiles 6-5, 9-2
Users 6-4
Validation 9-2

Validation 9-2
Vertical Markets 2-3
Viewlets 3-5, 6-3
Views
Topology Browser 6-6

Web Consoles 3-5, 6-3
webconsole.properties 8-5