EMC® Smarts®

7.0

Quick Start Guide

P/N 300-004-060
REV A01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 2006 EMC Corporation. All rights reserved.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

EMC Smarts 7.0 Quick Start Guide

This guide provides quick start tasks and procedures for EMC® Smarts® IP and Service Assurance Manager software products. This guide contains the following information:

- A basic deployment 2
- Installing the software 4
- After you install the software 5
- Before you use the IP software 8
- Before you use the Service Assurance Manager software 10
- Using the Global Manager 12

A basic deployment

Figure 1-1 illustrates a basic EMC Smarts deployment. The deployment consists of the following suites and components.

- Availability Manager — Diagnoses connectivity failures in multivendor, switched, and routed networks.
- Performance Manager — Monitors the performance of Layer 2 and Layer 3 network elements in switched and routed networks.
- Adapter Platform — Imports SNMP traps and topology and event information from third-party applications or products, normalizes the imported data to the InCharge Common Information Model (ICIM), and provides the data to the Global Manager.
- Global Manager — Consolidates topology and event information from multiple underlying domains and provides a central point for monitoring and managing distributed analysis domains.
- Global Console — Enables network operations personnel to monitor the state of the managed environment and quickly respond to notifications.

Note: Additional applications, custom products, and advanced networking solutions can be integrated with the basic deployment, but are not covered in this Quick Start Guide.

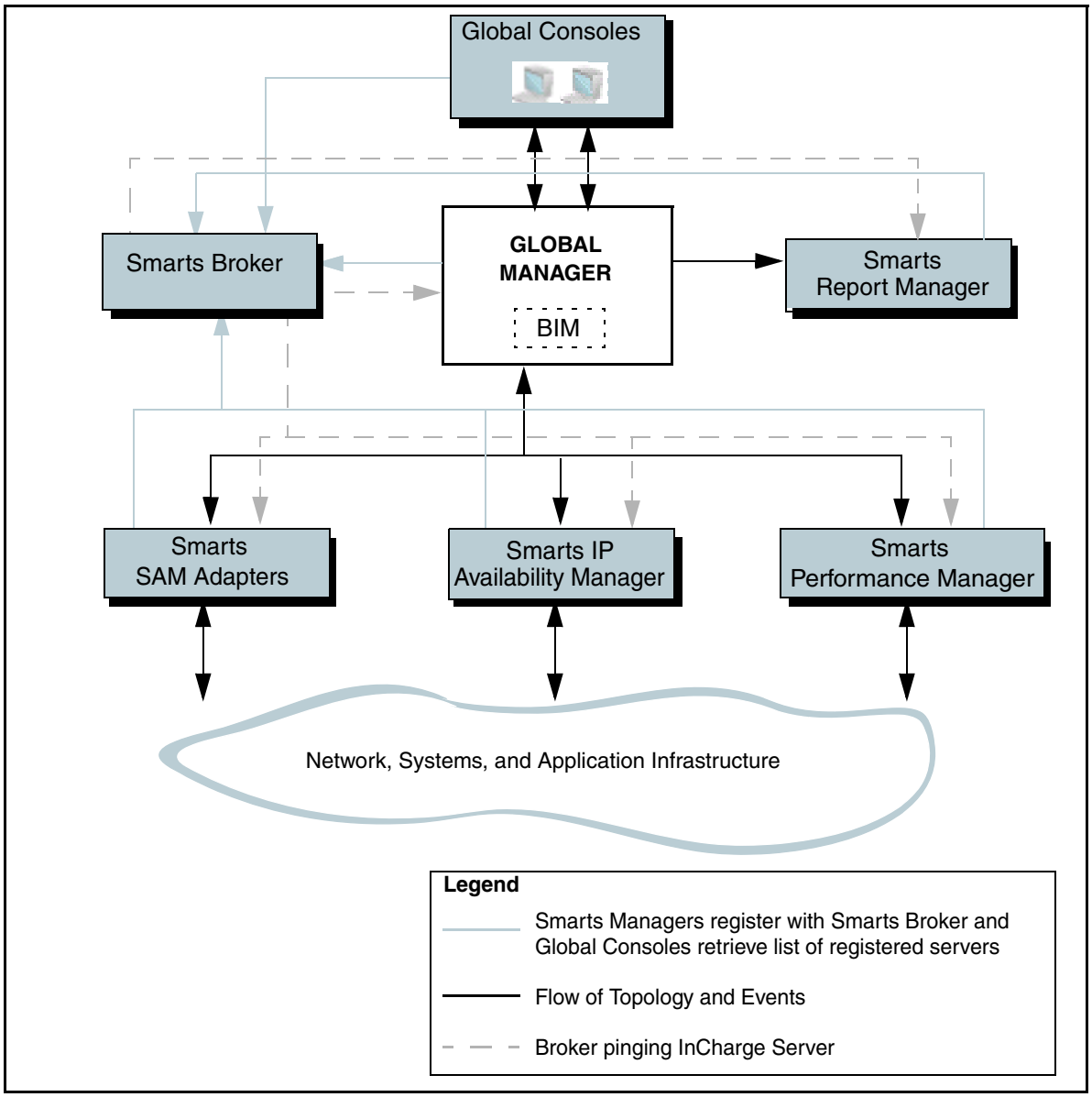

Figure 1-1 **A basic EMC Smarts deployment**

For all deployments, have the following information available before you install the software, the:

- Host machine(s) hardware and software configurations
- Installation locations
- Name and port of the broker
- Location of the license server and license

Installing the software

Most EMC Smarts software is installed with the following steps:

1. Insert the CD-ROM and execute Installation Setup.

   Note: To install the software on a UNIX system, mount the CD-ROM.

2. Install the EMC Smarts Suites, SmartPack, and Rolling Patches.
3. Remove the CD-ROM.

See the installation guide(s) for your product(s) for detailed information.

Note: Some EMC Smarts products are downloaded from EMC Powerlink™. To install a downloaded product, follow the procedures provided with the software.

After you install the software

Licensing

License files are not included with EMC Smarts software.

To obtain a license file, send an email request to smartslicensing@EMC.com or contact your sales representative. Indicate whether you need a temporary (evaluation) or a permanent license file.

- If you request a temporary license file, a sales representative will contact you.
- If you request a permanent license file, EMC Corporation will send you an email with an attached Permanent License Information Request form to complete.

For a temporary license file, complete an evaluation request and evaluation agreement. EMC Corporation sends you an email with an attached temporary license file shortly after the software is shipped.

For a permanent license file, you will need to complete a Permanent License Information Request form. On this form, please supply:

- The host ID of the computer where the FLEXnet license server is or will be running
- The hostname
- The EMC Smarts software version
- The expected installation path to BASEDIR/smarts/bin for the EMC Smarts installation from which you want to run the license server
- EMC Smarts products to enable
- The number of managed devices

After you purchase the software, EMC Corporation sends you an email with an attached permanent license file.

The *EMC Smarts System Administration Guide* contains detailed information about installing the licenses.

Starting the products as services

EMC Smarts programs (and their components) installed as services start automatically upon system reboot; reboot the system or start the services manually.

Starting services on UNIX

To start services manually, use the sm_service utility:

```
sm_service start <service_name> [<service_name> ...]
```

For example, to start EMC Smarts Service Assurance Manager as a service, enter the following:

```
# BASEDIR/smarts/bin/sm_service start ic-sam-server
```

Starting services on Windows

Use the Service control panel (Settings > Control Panel > Administrative Tools > Services) to start the services, or start them with the sm_service utility.

See the installation guide(s) for your product(s) for detailed information.

Setting up security

By default, encryption is enabled during the installation process. The basis for encryption is a secret phrase (by default, Not a secret) that gets transformed into the file imk.dat.

Changing the secret phrase

To change the secret, perform the following:

- Use the sm_rebond utility.

  On UNIX, invoke the utility from the BASEDIR/smarts/bin directory.

  ```
  % sm_rebond --basedir=<base directory>
  ```

  On Windows systems, invoke the utility as follows.

  ```
  C:\>sm_rebond --basedir=<base directory>
  ```

  For the <base directory>, enter the path for the directory in which the EMC Smarts software to be rebonded is installed.

- When the utility prompts for the old secret phrase, enter it.
- When the utility prompts for the new secret phase, enter it.
- Reenter the new secret to confirm it, and close out of the utility.

The *EMC Smarts System Administration Guide* contains detailed information.

Changing encrypted passwords

To enter or change a password in a configuration file, perform the following steps. The configuration files are located in the BASEDIR/smarts/local/conf directory of a product suite.

- Use sm_edit to open the file.

  For example, to open the serverConnect.conf file on UNIX, invoke sm_edit from the BASEDIR/smarts/bin directory:

  ```
  % sm_edit conf/serverConnect.conf
  ```

  To open the file on Windows systems, invoke sm_edit as follows:

  ```
  C:\>sm_edit conf\serverConnect.conf
  ```

- Review the contents of the file. For example, the serverConnect.conf file may include lines similar to the following.

  ```
  #
  <BROKER>    :<DEFAULT>:<DEFAULT>:All
  InCharge    :admin    :<SYS>    :All
  InCharge-WP :user5    :Password :Ping
  InCharge    :operator :Password :Monitor
  InCharge    :*        :<SYS>    :None
  #
  ```

  Encrypted passwords are preceded by <E-1.0>

- Delete the current password and replace it with the new password in plain text. If the current value is encrypted, delete the <E-1.0> tag that marks the password as encrypted as well as the current password. The special values <DEFAULT>, <PROMPT>, <SYS>, and <AUTO> in the files are not encrypted.
- Save the file and close it.

  When you save and close the file with sm_edit, the appropriate values are encrypted as part of the process.

Repeat the steps for all of the configuration files (serverConnect.conf, clientConnect.conf, and brokerConnect.conf).

Before you use the IP software

Before using the EMC Smarts IP Management Suite, discover the network topology. There are three methods for discovering the network infrastructure, using the:

- Import from seed file command
- Add Agent command
- Autodiscovery

Note: Using autodiscovery is the recommended method.

Using autodiscovery

Autodiscovery is configured and initiated through the Domain Manager Administration Console. ("Using the Global Manager" on page 12 includes information on accessing the Global Console. When the Notification Log Console opens, select Configure > Domain Manager Administration Console.)

To use autodiscover, complete the following steps:

1. Create one or more discovery filters.
2. Enable autodiscovery.
3. Initiate autodiscovery.

Creating one or more discovery filters

Follow the steps below to create one or more discovery filters:

1. In the left panel of the **Domain Manager Administration Console**, click the Domain Manager name. A multiple-tab window appears in the right panel of the console.
2. Click the **Discovery Filters** tab.
3. Specify values for each of the discovery filter fields.
4. Decide whether newly discovered systems matching this filter should be added to the topology automatically.
5. Click **Add**.
6. Click **Apply**.

Enabling autodiscovery

Follow the steps below to enable autodiscovery:

1. In the left panel of the **Domain Manager Administration Console**, click the Domain Manager name to display a multiple-tab window in the right panel of the console.
2. Click the **Topology** tab.
3. Select the **Enable Auto Discovery** checkbox.
4. Select the data sources that discovery should use to find additional candidate systems.

5. In the **Community String** field, provide any additional read community strings necessary to communicate with systems on your network.
6. In the **Current System Limit** field, enter the total number of systems you want to allow into the topology.
7. Click **Apply**.

Initiating autodiscovery

To start the autodiscovery process:

1. Specify one or more seed systems using the **Import from seed file** command, or specify a single seed system (routers and switches make good seed systems) using the **Add Agent** command.
2. Initiate discovery.

The *EMC Smarts IP Management Suite Discovery Guide* contains additional information.

Before you use the Service Assurance Manager software

EMC Smarts software is installed with default configuration parameters that provide a base from which you can tailor it to meet the needs of your environment.

Configuration of the Global Manager is accomplished using several different methods:

- Editing the ics.conf configuration file
- Using the Global Manager Administration Console
- Using the sm_config utility

The following sections outline the configuration tasks. The *EMC Smarts Service Assurance Manager Configuration Guide* contains detailed information.

To configure the software, you can:

- Specify underlying domains and system-wide parameters
- Create user profiles
- Define the management of notifications and topologies

Configuring system parameters

System configuration includes tasks that define the operation of the Global Manager, including:

- Specifying sources of topology and events
- Defining the interaction between the Global Manager and Global Consoles
- Defining the interaction between the Global Manager and underlying domains

Specify the domains and the parameters that control the import of event and topology data in the DomainSection of the ics.conf configuration file. The file, which consists of several sections, is located in the BASEDIR/smarts/conf/ics directory and should be edited using the sm_edit utility.

The following example illustrates the syntax for one section of the ics.conf file. The DomainSection is composed of two DomainType subsections for Domain Managers called INCHARGE-AM and INCHARGE-OI.

```
DomainSection
{
# DomainType definition for INCHARGE-AM.
DomainType
{
ConfFile = "dxa-conn.conf";
MinimumCertainty = 0.24;
SmoothingInterval = 65;
# HookScript = "ics/dxa-sample-hook.asl";
Name = "INCHARGE-AM";
}
# DomainType definition for INCHARGE-OI.
DomainType
{
ConfFile          = "dxa-oi.conf";
MinimumCertainty  = 0.24;
SmoothingInterval = 65;
# HookScript = "ics/dxa-sample-nl-hook.asl";
Name              = "INCHARGE-OI";
}
```

Creating user profiles

A user profile defines the environment for one or more users; that is, anyone who requires access to the Global Managerr through the Global Console. You can create user profiles based on role (administrator/operator), job function (network management/helpdesk), or a combination of these and more.

Create user profiles with the Global Manager Administration Console or by using the sm_config utility. From the Global Manager Administration Console, choose Edit > New User Profile or click the Launch User Profile Wizard toolbar button.

Managing topology and notifications

Managing the topology and notifications maintained by the Global Manager requires:

- Organizing managed elements into groups. Groups are created and edited through the Group Definition window. Open this window by selecting Groups from the Configure menu of the Global Console.
- Creating notification lists. You can limit the set of notification types operator's will view on the console. Use the Global Administration Console to create notification lists. The *EMC Smarts Service Assurance Manager Configuration Guide* contains detailed information.
- Customizing operator consoles. You can:
  - Modify the look and feel of the console
  - Restrict access to some menus and tools
  - Assign a notification list
  - Move columns
  - Add summary views, status tables, and maps
  - Save the layout of the console

The *EMC Smarts Service Assurance Manager Configuration Guide* contains detailed information.

Using the Global Manager

The following sections highlight accessing the Global Console. The *EMC Smarts Service Assurance Manager Operator's Guide* contains detailed information.

Opening the Service Assurance Global Console

The Service Assurance Global Console is available for use in both UNIX and Windows environments.

Opening the console in a UNIX environment

To start a new session and open a new console in a UNIX environment, use the sm_gui command:

```
% BASEDIR/smarts/bin/sm_gui
```

Opening the console in a Windows environment

To start a new session and open a new console in a Windows environment:

1. Click the **Start** button in the Windows Taskbar.
2. Select **Programs** > **InCharge7** > **Global Console**.

Attaching to a Domain Manager

Before the console appears, a dialog box prompts you to attach to a Domain Manager and log on.

- The dialog box displays the broker hostname and port number values (that were provided during the installation process). You may need to change them. The default is localhost:426.
- Select a Service Assurance Domain Manager in the Manager list, or click the Browse button to display a list of active (running) Domain Managers and select one.
- Enter your username and password, and click OK to display the console.