## Table of Contents

**Preface** 7

- Audience .................................................. 7
- About This Guide ........................................ 7
- Revision Information ...................................... 8
- Documentation Conventions ......................... 8
- Technical Support ......................................... 9
- Professional Services ................................. 9

### Chapter 1  eHealth — System and Application Overview 11

- Benefits of eHealth — System and Application ........ 11
- Managing Systems and Applications .................. 12
  - Managing Systems .................................. 13
  - Managing Applications ............................. 14
- Overview of eHealth — System and Application ........ 14
  - eHealth SystemEDGE ............................... 15
  - eHealth AIMS ....................................... 15
  - eHealth AdvantEDGE View ......................... 16
  - eHealth ............................................. 17
- Supplementing eHealth — System and Application .... 18
  - eHealth Reports ................................... 18
  - eHealth Live Health ............................... 18
  - eHealth Service Availability .................... 19
  - eHealth — Network ................................ 19
  - eHealth — Response .............................. 19
# Table of Contents

## Chapter 2  Managing and Monitoring Systems  21
- Collecting System Data ........................................ 21
- Using the SystemEDGE Agent To Manage and Monitor Systems ............................................... 22
- Using AdvantEDGE View To View System Data and Manage SystemEDGE Agents .......................... 27
- Using eHealth To Collect and Report on System Data ................................................................. 36
- eHealth Reports for Systems .................................... 42
  - At-a-Glance Reports for Systems .......................... 44
  - Trend Reports for Systems ................................. 46
  - Top N Reports for Systems ................................. 48
  - What-If Capacity Trend Reports for Systems .......... 48
  - MyHealth Reports for Systems .......................... 49
  - Health Reports for Systems .............................. 49
  - Service Level Reports for Systems ....................... 51

## Chapter 3  Configuring System Process Sets  53
- Configuring System Process Sets ............................ 53
- Monitoring an Application’s Effects on a System ........ 53
- Defining Process Sets ........................................ 54
- Using Process Sets Effectively ............................... 54
- Using Discover Rules To Discover Process Sets ........ 55
- Creating a Process Set for an Application .................. 56
- Deleting a Process Set Definition ............................ 62
- Example: Creating a Process Set ............................ 63
- Sample Reports for Process Sets ............................ 67
- Troubleshooting Systems .......................... 69
- Resolving Errors in Polling ................................. 69
- Resolving Excessive Use of Disk Space by SystemEDGE Log Files ........................................ 69
This guide describes eHealth® — System and Application. It provides an overview of the features that are available with each component of eHealth — System and Application, as well as some detailed configuration information. This guide supports eHealth Release 5.6 and later.

**Audience**

This guide is intended for an administrator or Information Technology (IT) manager who is planning to use eHealth — System and Application to monitor systems and applications. It requires a basic understanding of system and networking concepts. It does not require previous knowledge of, or experience with, eHealth. For an overview of how eHealth — System and Application relates to the other eHealth products, refer to the Introduction to eHealth guide.

**About This Guide**

This guide also provides information about how you can use eHealth SystemEDGE™, eHealth AdvantEDGE View, and the eHealth application insight modules (AIMs) to monitor systems and applications, but it does not provide detailed configuration instructions for these products. For more information, refer to the eHealth SystemEDGE User Guide, eHealth AdvantEDGE View User Guide, or the user guide for the eHealth AIM that you are using.
This section describes the guide’s revision history and the documentation conventions used in this guide.

Revision Information
This is the first release of this guide, which combines information that previously existed in the System Health Administration Guide and the Application Health Administration Guide.

Documentation Conventions
Table 1 lists the conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or Directory Name</td>
<td>Text that refers to file or directory names.</td>
</tr>
<tr>
<td>code</td>
<td>Text that refers to system, code, or operating system command line examples.</td>
</tr>
<tr>
<td>emphasis</td>
<td>Text that refers to guide titles or text that is emphasized.</td>
</tr>
<tr>
<td>enter</td>
<td>Text that you must type exactly as shown.</td>
</tr>
<tr>
<td>Name</td>
<td>Text that refers to menus, fields in dialog boxes, or keyboard keys.</td>
</tr>
<tr>
<td>New Term</td>
<td>Text that refers to a new term, that is, one that is being introduced.</td>
</tr>
<tr>
<td>Variable</td>
<td>Text that refers to variable values that you substitute.</td>
</tr>
<tr>
<td>→</td>
<td>A sequence of menus or menu options. For example, File → Exit means “Choose Exit from the File menu.”</td>
</tr>
</tbody>
</table>

Table 1. Documentation Conventions  (Page 1 of 2)
Table 1. Documentation Conventions  (Page 2 of 2)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE</strong></td>
<td>Important information, tips, or other noteworthy details.</td>
</tr>
<tr>
<td><strong>CAUTION</strong></td>
<td>Information that helps you avoid data corruption or system failures.</td>
</tr>
<tr>
<td><strong>WARNING</strong></td>
<td>Information that helps you avoid personal physical danger.</td>
</tr>
</tbody>
</table>

**Technical Support**

If you have a Support Contract ID and password, you can access our Support Express knowledgebase at the following URL: http://search.support.concord.com.

If you have a software maintenance contract, you can obtain assistance with eHealth. Have your Support Contract ID available and contact Technical Support at the following:

- **Phone:** (888) 832-4340
- (508) 303-4300
- **E-mail:** support@concord.com
- **Web site:** http://www.concord.com

**Professional Services**

If you need any assistance with customizing this product, contact Professional Services at the following:

- **Phone:** (800) 851-8725
- **Fax:** (508) 486-4555
- **E-mail:** proserv@concord.com
- **Web site:** http://www.concord.com
eHealth — System and Application

Overview

eHealth® — System and Application is a product set that manages and monitors the availability and performance of critical systems and applications. It helps automate system and application management by shifting the workload from IT personnel to intelligent, self-monitoring agents on distributed systems. eHealth — System and Application also provides detailed reports that can give you a historical view of system and application performance for trend analysis, capacity planning, and troubleshooting. It provides a comprehensive view of your systems and the applications that are running on them.

Benefits of eHealth — System and Application

You can use eHealth — System and Application to do the following:

- Manage thousands of heterogeneous systems without increasing your existing staff.
- Automate the management of critical systems and applications.
- Document service levels and plan capacity across large, distributed environments.
- Gain control of your investment through automated asset tracking.
- Detect real-time faults and events across systems and applications.
Perform trend analysis, capacity planning, and proactive, real-time self-management.

Protect your investment in management software; SystemEDGE works with most SNMP management applications, including Aprisma® SPECTRUM™, HP® OpenView, Sun™ Enterprise Manager, and Tivoli® NetView™.

Provide consistent management across operating systems, including Solaris™, HP-UX™, Linux, Compaq® Tru 64, Windows®.

Managing Systems and Applications

Discover is the process by which eHealth searches for devices, obtains information, and creates elements based on that information.

eHealth — System and Application consists of the following products, which are described in “Overview of eHealth — System and Application” on page 14:

- SystemEDGE™ agent
- eHealth AIMS
- AdvantEDGE™ View
- eHealth

You can use the products of eHealth — System and Application to discover, monitor, and manage systems and their associated resources, as well as the applications that are running on those systems. When you are managing systems and applications, you need to monitor performance and detect and respond to errors before they have a negative impact on your systems and applications.

Most systems can support a variety of applications. Applications typically consist of one or more processes that perform various functions and consume CPU and other system resources. Monitoring the impact of an application and its processes is an important part of determining whether a system can support the application effectively. If a system cannot support the application, users experience delays and problems while using the application.

A system is a server or client computer on which users install software products. An application is a software program that you install on a system to provide services for one or more client users.
A process set is a collection of one or more processes that relate to a specific application.

Most systems track the impact of individual processes on the system. To monitor the impact of all processes that relate to an application, you must associate them with the application. With eHealth, you can create a process definition to associate all of the processes that you want to monitor as a single application. eHealth also enables you to specify the process sets that it can discover. After polling the processes, eHealth aggregates the data for the associated process set.

After eHealth discovers applications, it creates application service elements, which represent monitored applications that reside on a system that the SystemEDGE agent is monitoring. eHealth also creates application service process sets, which represent the footprint information for application service elements. You can run eHealth reports on these system and application process set elements.

**Managing Systems**

To manage system performance effectively, you must monitor the system’s resource utilization, such as memory, disk space, central processing unit (CPU), network input/output (I/O), and disk I/O. Your systems must have sufficient resources to support the applications and their users.

You must also identify and correct errors before they interfere with the performance of your system. Errors are often indicators that systems are failing or are configured incorrectly. For example, disk errors can indicate that a disk is beginning to fail. By detecting increases in the number of errors, you can make plans to replace the disk before it fails completely.

In addition, you must track your assets so that you can plan upgrades and service profiles that are specific to your system. In today’s growing and changing internet infrastructure, your inventory can change frequently as you add new systems, perform system upgrades, and apply new patches. You need to keep a current inventory of your systems, their configuration, and their operating system platforms in order to manage those systems effectively.
eHealth — System and Application enables you to manage all of these areas and to automate management tasks. It also helps you manage the critical applications that reside on your systems.

Managing Applications

When you monitor applications, the criteria that you want to track varies according to the type of application you are monitoring. For most applications, you will want to monitor the amount of CPU, disk space, and memory that they are consuming. You may also want to monitor other criteria that are specific to the type of application you are monitoring. For example, for e-mail applications like Microsoft Exchange, you might want to monitor the number of messages and bytes processed. For databases like Oracle and Microsoft SQL Server, you might want to monitor log files and backup status.

eHealth — System and Application enables you to collect performance and configuration data for a variety of critical applications. You can run reports on this data for real-time analysis, and you can save the data for future historical analysis.

Overview of eHealth — System and Application

When you use the products that comprise eHealth — System and Application with an eHealth — System license, you can discover and poll systems, run eHealth reports, and perform Live Health real-time monitoring on critical system metrics such as CPU utilization, disk space, memory, and paging. If you use these products with an eHealth — Application Insight license, you can discover and poll applications that are installed on systems that use eHealth SystemEDGE and one or more eHealth AIMs. You can run reports and perform real-time monitoring of your critical application metrics. If you use both licenses, you can gain valuable information about not only the application performance, but also its impact on the system and overall health of the system on which it runs.
This chapter provides an overview of the components of eHealth — System and Application. The following chapters provide additional information about those components and how you can use them together.

**eHealth SystemEDGE**

At the core of eHealth — System and Application is the SystemEDGE agent, the intelligent, self-managing, Simple Network Management Protocol (SNMP) agent that collects data on system performance and availability. The SystemEDGE agent operates autonomously on workstations or servers, continuously monitoring changing conditions in real time and alerting you to situations that require attention. It can also automatically fix problems or potential problems when you configure actions.

Because SystemEDGE is an SNMP agent, you can integrate it with other management systems. SystemEDGE works with any SNMP management software, but AdvantEDGE View and the eHealth console are optimized to work with SystemEDGE.

The SystemEDGE agent is also extremely efficient, using less than 1% of CPU and about 3 MB of memory. With such a small footprint, it does not affect system performance, even on low-end servers and workstations. For more information about SystemEDGE, refer to Chapter 2, “Managing and Monitoring Systems.”

**eHealth AIMs**

*eHealth AIMs* are plug-in modules for the SystemEDGE agent that provide the capability to monitor and manage application-specific events and processes. Each eHealth AIM is designed to monitor a specific application. For example, the eHealth AIM for Microsoft Exchange enables monitoring of the Microsoft Exchange e-mail application. When the SystemEDGE agent loads this eHealth AIM, it can begin to collect...
information about disk capacity; the number of messages and bytes processed; and overall CPU and physical memory utilization for Microsoft Exchange. The following eHealth AIMs are currently available for application management:

- eHealth AIM for Apache
- eHealth AIM for Check Point™ FireWall-1™
- eHealth AIM for Microsoft® Exchange
- eHealth AIM for Microsoft IIS
- eHealth AIM for Microsoft SQL Server
- eHealth AIM for Network Services for UNIX
- eHealth AIM for Network Services for Windows
- eHealth AIM for Oracle®

For more information about the eHealth AIMs, refer to Chapter 4, “Managing and Monitoring Applications.”

**eHealth AdvantEDGE View**

AdvantEDGE View is the Web-based graphical user interface and element manager that can receive and report on data that the SystemEDGE agent and the eHealth AIMs collect. AdvantEDGE View can also automate the licensing, deployment, and configuration of your SystemEDGE agents and eHealth AIMs. It is available as an integrated part of the eHealth Web interface and as a standalone element manager.

**NOTE**

This guide discusses AdvantEDGE View as an embedded part of the eHealth Web interface. For information about the standalone version of AdvantEDGE View, refer to the eHealth AdvantEDGE View User Guide.

For more information about AdvantEDGE View, refer to Chapter 2, “Managing and Monitoring Systems.”
eHealth

While the SystemEDGE agent, AdvantEDGE View, and the eHealth AIMs provide a real-time view of your systems and applications, eHealth provides the long-term, historical view that is essential for trend analysis, capacity planning, and proactive troubleshooting.

You can configure the eHealth poller to collect performance and availability data for thousands of workstations and servers across different operating systems. The poller can collect this data from SystemEDGE agents and from many other certified SNMP agents. For a complete list of certified devices that eHealth can manage using eHealth — System and Application, refer to the Device and Technology Certification page of the Concord Corporate Web site at http://www.concord.com.

eHealth stores the collected data in the eHealth database and makes it available to reporting and real-time monitoring tools. After eHealth stores the data, you can run At-a-Glance, Trend, Top N, What-If Capacity Trend, and MyHealth reports for your systems and applications to perform capacity planning, accurately document service levels, and troubleshoot potential problems. If system or application performance looks questionable, you can drill down for more performance details to pinpoint the source of performance problems. For example, if you notice high CPU utilization on a server, you can drill down to a report that identifies the applications that use the most CPU. For more information about eHealth and the reports that it provides, refer to “eHealth Reports for Systems” on page 42.
Supplementing eHealth — System and Application

To supplement the features of eHealth — System and Application, you can purchase the following:

- Health Report and Service Level Report licenses
- eHealth Live Health™
- eHealth Service Availability
- eHealth — Network
- eHealth — Response

**eHealth Reports**

eHealth — System and Application provides the following standard reports: At-a-Glance, Trend, Top N, What-If Capacity Trend, and MyHealth. You can also purchase additional report licenses for Health Reports and Service Level Reports. These reports can help you track the performance of groups of elements and look for situations that might require attention. They can also help you summarize performance by enterprise, region, department, or business unit. For more information, refer to “eHealth Reports for Systems” on page 42.

**eHealth Live Health**

You can also purchase an eHealth Live Health license and use eHealth — System and Application with Live Health to define system thresholds and to detect potential outages and delays that can cause downtime and service degradation. For example, you can use Live Exceptions profiles to detect service delays without having to configure complicated rules. In this way, you can correct potential problems before your users notice any performance differences. You can use Live Health — Fault Manager to receive traps from SystemEDGE agent and to take actions based on Live Exceptions alarm rules. For more information about Live Health, refer to the eHealth Live Health Administration Guide.
eHealth Service Availability

eHealth Service Availability is a plug-in module for the SystemEDGE agent that provides active testing of system, application, and network performance. It initiates repeatable test transactions at specified intervals to detect changes in performance and availability. For more information, refer to the eHealth Service Availability User Guide.

eHealth — Network

eHealth — Network helps you analyze and measure the performance of networks, including LAN/WAN interfaces, remote-access devices, routers, switches, network traffic, and QoS-enabled devices. It provides reports on bandwidth utilization, traffic patterns, error conditions, and network performance. For more information, refer to the Network Health Administration Guide.

eHealth — Response

eHealth — Response collects response time data from a variety of sources for real-time analysis, historical reporting, and service-level management. You can use eHealth — Response to monitor and manage the performance and availability of applications and services in your infrastructure. You can also report on network activity between Cisco® routers and other devices. eHealth — Response offers a comprehensive set of reports that you can use to manage your critical services and applications. For more information, refer to the eHealth — Response Administration Guide.
Managing and Monitoring Systems

This chapter provides an overview of how you can use the SystemEDGE agent, AdvantEDGE View, and eHealth to manage and monitor your systems. For detailed information about configuring and using those products, refer to the eHealth SystemEDGE User Guide, the eHealth AdvantEDGE View User Guide, and the eHealth Administration Guide.

Collecting System Data

You can use the SystemEDGE agent with AdvantEDGE View and eHealth to provide a comprehensive view of your systems and to manage them for optimal productivity. The SystemEDGE agent enables you to control all workstations on your networks from a single, central location. It enables you to automate systems-management tasks and inventory tracking. AdvantEDGE View provides an intuitive graphical interface to the SystemEDGE agent, enabling you to easily configure the agent’s self-monitoring capabilities and provide detailed reports on the data collected by the agent.

eHealth provides a console and Web interface through which you can collect data, and monitor and report on system performance. It also provides the long-term, historical view that is essential for trend analysis, capacity planning, and proactive troubleshooting.
With the SystemEDGE agent, AdvantEDGE View, and eHealth, you can increase productivity and system stability while reducing system-support costs.

**Using the SystemEDGE Agent To Manage and Monitor Systems**

The SystemEDGE agent enables remote management systems to access important information about systems through SNMP. It also includes intelligent self-monitoring capabilities for scalable management (including detection, notification, and repair) of attributes, thresholds, processes, log files, and exceptions. The SystemEDGE agent provides detailed information about the system’s configuration, status, performance, users, applications, file systems, and other critical resources.

**Collecting Data**

You must install the SystemEDGE agent on every workstation or server that you want to monitor. You can then configure SystemEDGE to monitor those systems for variables that you specify. SystemEDGE supports monitoring objects from the following Management Information Bases (MIBs):

- MIB-II (RFC 1213), the standard that provides information about the network interface and protocol statistics.
- Host Resources MIB (RFC 1514), which defines objects for monitoring host computers.
- Systems Management MIB, a Concord private-enterprise MIB, which includes the monitoring tables that you can use to configure the SystemEDGE agent’s self-monitoring and data-storage capabilities, as well as objects for monitoring the health and performance of the underlying system and its applications.

For more information about these MIBs, refer to the eHealth SystemEDGE User Guide.
SystemEDGE Self-Monitoring Features

When you manage a large enterprise network with hundreds of systems, you may need to place limits on the information and number of systems that your agents are monitoring, and on the poll rate. The unique self-monitoring capability of the SystemEDGE agent is specifically designed to provide the kind of management by exception that is necessary in distributed network environments.

The SystemEDGE agent can monitor the following:

- Thresholds
- Processes and Windows services
- Process groups
- Log files
- Windows events

SystemEDGE also provides history collection. You can configure these self-monitoring features by adding entries to the monitoring tables of the Systems Management MIB. You can add these entries manually to the sysedge.cf file, or you can use AdvantEDGE View or another element manager to edit the sysedge.mon file with SNMP Sets.

Threshold Monitoring. The SystemEDGE agent can monitor exception conditions automatically, reducing or eliminating the need for constant polling by a network management system (NMS). You can configure the agent’s flexible Monitor table to monitor any integer-based MIB object that the agent supports. You set the polling interval, comparison operator (greater than, equal to, and so on), and threshold value, and SystemEDGE automatically monitors the MIB objects that you specify. You can tailor entries for time over threshold to reduce noise. The SystemEDGE agent can also send traps to an NMS if exceptions occur.

For example, you can configure the SystemEDGE agent to monitor the available space on a particular file system and to notify the NMS when the file system becomes too full.
**Process and Windows Service Monitoring.** The SystemEDGE agent can monitor process attributes for mission-critical processes, applications, and Windows services. It can monitor attributes such as the status (whether the process is running), network I/O, and system calls. If any processes stop running, SystemEDGE can automatically notify the NMS and restart them, if necessary. You can configure both process and Windows service monitoring by adding entries to the Process Monitor table of the Systems Management MIB.

**Process Group Monitoring.** With the SystemEDGE agent, you can monitor process groups to determine what processes exist in each group and whether the group membership changes. If components of an application start or fail, or if members leave a group or are added to a group, SystemEDGE can automatically notify the NMS. You can configure the SystemEDGE agent to monitor process groups in the Process Group Monitor table.

**Log File Monitoring.** You can use SystemEDGE to monitor any system or application log file for regular expressions. For example, you can configure the SystemEDGE agent to monitor the log file `/var/adm/sulog` for any regular expression by adding an entry for that expression to the Log Monitor table of the Systems Management MIB. Whenever a message that matches the regular expression you have specified is logged to the file, the SystemEDGE agent notifies the NMS through an SNMP trap and includes the log entry that matched the expression.

**Windows Event Monitoring.** The SystemEDGE agent can also monitor Windows event logs for important event types, event identifiers, or events that match specific regular expressions. This feature is similar to the log file monitoring feature, but it provides more specific searches for characteristics of Windows events. You can specify the search criteria in the NT Event Monitor table of the Systems Management MIB; when an event that matches the search criteria occurs, the SystemEDGE agent notifies the NMS through an SNMP trap.
**History Collection.** You can configure the SystemEDGE History Control table to sample MIB variables, such as load average and CPU utilization, and to use the collected data for baselining and trend analysis of your system without having to constantly poll from the NMS. SystemEDGE collects the data, and the NMS can periodically retrieve the history.

*NOTE*

The SystemEDGE history collection capability is short-term only; it stores the data in memory. For long-term history collection, use eHealth. For more information, refer to “Using eHealth To Collect and Report on System Data” on page 36.

**Identifying Top Processes**

The SystemEDGE agent provides a flexible architecture that supports the addition of plug-in modules for monitoring processes and applications. One of these plug-ins is the Top Processes module, through which the agent can report on processes that are consuming the greatest amount of CPU resources at any given time. After you use Top Processes to detect and isolate the CPU-dominating processes, you can immediately reallocate resources to ensure optimal system and application availability and performance.

**Tracking Assets**

The SystemEDGE agent can automate asset tracking and can provide an up-to-date picture of your installed hardware and software by determining whether your systems are properly configured and whether they include the current patches and service packs. This information can help simplify system management, improve performance, and reduce security risks. For more information, refer to the chapter on the Host Resources MIB in the *eHealth SystemEDGE User Guide*.

*eHealth — System and Application Administration Guide*
Specifying Corrective Actions

You can configure SystemEDGE to perform corrective actions through the use of traps and the SystemEDGE self-monitoring features. For example, you can specify a script or program to run when monitor thresholds are crossed, when log file monitor matches are discovered, and when Windows NT event matches occur.

You can use action commands to perform the following types of tasks:

- Send e-mail to one or more addresses to notify system administrators that a critical event has occurred.
- Page a system administrator when a critical event occurs.
- Check on the status or size of a file and return its size, or report that the file does not exist.
- Automatically restart critical processes and services when they fail.
- Clean up file systems when they are full.
- Reboot Windows systems when they are not responding.

Supporting Custom MIB Objects

The SystemEDGE agent enables you to add your own scalar MIB objects for customized management. You can configure the SystemEDGE agent with each object’s number and type, and with the name of a script or program to execute when the new MIB variable is queried or set.

Supporting Windows Registry and Performance-Monitoring Extensions

You can configure the SystemEDGE agent for Windows to report additional registry parameters and performance data without using external programs or scripts. This feature allows you to use the performance registry to monitor the health of applications that make performance data available. For more information about using Windows and performance MIB
objects, refer to eHealth SystemEDGE User Guide. You can also monitor applications with existing eHealth AIMs. For more information, refer to “Using the SystemEDGE Agent and eHealth AIMs To Collect Application Data” on page 73.

Using AdvantEDGE View To View System Data and Manage SystemEDGE Agents

AdvantEDGE View provides an intuitive graphical user interface for deploying, configuring, and licensing the SystemEDGE agent and eHealth AIMs, as well as for reporting on data collected by the SystemEDGE agent and eHealth AIMs. This section describes the features that are available with AdvantEDGE View from the eHealth Web interface. If you are using the standalone version of AdvantEDGE View, refer to the eHealth AdvantEDGE View User Guide for more information.

You can use AdvantEDGE View from the eHealth Web interface to do the following:

- Report on the real-time status of critical systems and applications.
- Deploy, configure, and license SystemEDGE agents and eHealth AIMs.
- Access configuration information for systems or groups.
- Define and apply SystemEDGE configuration templates.
- Receive and process event notifications (traps) that originate from SystemEDGE agents (unless you are using Fault Manager with eHealth).

To access the AView tab on the eHealth Web interface:

1. Start your Web browser, and enter the IP address or hostname of the system on which you are running eHealth. For example, if you are running eHealth on the system named aview, enter the following:

   http://aview

   The eHealth Welcome page appears.
2. Enter your user name and password in the User Name and Password fields. The eHealth Web interface appears.

3. Click the AView tab. The AdvantEDGE View page appears.

**NOTE**

If you cannot access the AView tab, you may not have the correct license or permissions. Use the Administration tab to set your permissions. For more information, refer to the eHealth Web Administration Guide.

Figure 1 shows the AdvantEDGE View page of the eHealth Web interface.

**Performing Administration Tasks**

You can access AdvantEDGE View administration tasks by clicking the Administration icon. The AdvantEDGE View Administration page provides the following options from the AView tab of the eHealth Web interface:

- AdvantEDGE View Preferences
- Configuration/Diagnostics
- Agent Deployment
License Management
Template Management

AdvantEDGE View Preferences. You can use the AdvantEDGE View Preferences form to specify and save information such as your contact information, your licensing user name and password, proxy information, deployment drive, and information about the AdvantEDGE View server system. AdvantEDGE View uses this information for performing licensing and deployment tasks.

To view or modify AdvantEDGE View Preferences:
1. Click the Administration icon. AdvantEDGE View displays the Administration page.
2. Click the AdvantEDGE View Preferences icon. AdvantEDGE View displays the AdvantEDGE View Preferences form.
3. Complete this form, and then click Modify to save your changes.

Configuration and Diagnostics. AdvantEDGE View provides configuration information about the version of AdvantEDGE View and any eHealth AIMS that you have installed on your system. It also provides the locations of the log and trap directories, and information about the AdvantEDGE View HTTP process. You can use this information for diagnostic purposes.

To view configuration information:
1. Click the Administration icon. AdvantEDGE View displays the Administration page.
2. Click the Configuration/Diagnostics icon. AdvantEDGE View displays the AdvantEDGE View Configuration form.
Deploying Agents and eHealth AIMs. You can deploy SystemEDGE agents, Application Response (AR) agents, and eHealth AIMs with the AdvantEDGE View Deployment Manager.

To deploy agents and eHealth AIMs from AdvantEDGE View:

1. Click the Administration icon. AdvantEDGE View displays the Administration page.
2. Click the Agent Deployment icon. AdvantEDGE View displays the AdvantEDGE View: Agent Deployment form.
3. Complete this form. AdvantEDGE View displays a list of systems that are eligible for deployment. If you selected one of the licensing options on the Agent Deployment form, the Licensing Account Information form also appears.
4. Deselect the check boxes in the Deploy? column for any systems to which you do not want to deploy the agents or eHealth AIMs; then click Deploy to Selected Hosts to begin the deployment.

AdvantEDGE View deploys the agents or eHealth AIMs to the systems that you selected and licenses them if you selected the licensing options and specified a valid licensing user name and password. For details about deploying the eHealth agents and eHealth AIMs, refer to the eHealth AdvantEDGE View User Guide or Web Help. For more information about AR agents, refer to the eHealth — Response Administration Guide

Creating and Applying Configuration Templates. You can create, modify, and deploy configuration templates for the SystemEDGE agent. Templates are text files that contain a series of configuration directives for SystemEDGE. Each template can include entries for any or all of the SystemEDGE self-monitoring tables. You can use the Template Manager to create, edit, copy, rename, and delete templates.
To access the Template Manager:

1. Click the Administration icon. AdvantEDGE View displays the Administration page.

2. Click the Template Management icon. AdvantEDGE View displays the Existing SystemEDGE Templates list.

3. Select New Template to create a template, or select a template from the Existing SystemEDGE Templates list, and then select one of the following options:
   - Edit Template
   - Copy Template
   - Rename Template
   - Delete Template

For details about performing these tasks, refer to the eHealth AdvantEDGE View User Guide or Web Help.

To apply templates to a system or group:

1. Select a target system or group from the System or Group list.

2. Select Template Configuration from the Configuration list.

3. Click the Configuration icon. AdvantEDGE View displays the Templates Installed list and the Templates Available for Installation list. If templates are not installed on that system, the Templates Installed list is blank.

4. Select the check box next to the name of the template you want to apply in the Available Templates to Install list, and click Apply Selected Templates. AdvantEDGE View applies the selected templates to the system that you selected, and displays a status message to let you know whether the application succeeded.
NOTE

You can also remove templates from a system or group by following this procedure, selecting the check box next to the name of the template that you want to delete in the Templates Installed list, and then clicking Unapply Selected Templates. AdvantEDGE View removes the selected templates from the system and refreshes the Templates Installed list.

Licensing SystemEDGE Agents and eHealth AIMs that eHealth discovered. If you used eHealth to discover system and application elements, it identifies any unlicensed SystemEDGE agents and eHealth AIMs. You can license them through AdvantEDGE View License Management. For information about discovering system elements, refer to “Discovering System Elements” on page 37.

To use the License Management form:

1. Click the Administration icon. AdvantEDGE View displays the Administration page.
2. Click the License Management icon. AdvantEDGE View displays a form that includes the system name, IP address, and the component that requires licensing.
3. Click the check box in the License column for the components that you want to license. You can select multiple check boxes to license multiple SystemEDGE agents and eHealth AIMs simultaneously.
4. Complete the License Account Info section of the form, and click License.

Handling Traps and Events

A trap is an SNMP event, or an unsolicited message that is delivered to a system. SNMP agents send trap messages to a console or NMS when specific conditions occur.
Use AdvantEDGE View event processing for small-scale processing of SystemEDGE events. For large-scale trap processing, use Fault Manager.

You can use AdvantEDGE View to view and filter events, and to clear traps. You can access the event-processing features of AdvantEDGE View by clicking the Events icon from the AdvantEDGE View interface or from the AView tab of the eHealth Web interface. For more information about processing events, refer to the eHealth AdvantEDGE View User Guide or the AdvantEDGE View Web Help.

NOTE

If you are using Live Health — Fault Manager, you cannot process events through AdvantEDGE View. Instead, you can use Fault Manager to define event rules that generate alarms when specific traps occur. For more information about using Fault Manager and the other Live Health tools with SystemEDGE and AdvantEDGE View, refer to Appendix A.

Querying SystemEDGE Agents

AdvantEDGE View provides quick, real-time queries on system data that is collected by the SystemEDGE agent, including memory usage, CPU utilization, disk and file system statistics, process and service information, and hardware and software inventories. You can use these queries to obtain configuration and performance information for each system or group, as well as real-time status of critical systems.

To run an AdvantEDGE View query:

1. Select the system or group that you want to query from the System or Group list of the AdvantEDGE View interface.

2. Select the query type from the Queries list.

3. Click the Queries icon.
Types of Queries. You can run the following types of queries:

- Configuration
  - System Information
  - Hardware Inventory
  - Software Inventory
  - Patch List
  - NT Event Log Info
  - History Sample

- Performance
  - Performance
  - CPU Statistics
  - Filesystems
  - Disk Statistics
  - Process Information
  - Top Processes
  - NT Services
  - NT Threads
  - Current Users
  - Extensions
  - NT Registry Extensions

- Network
  - Interface Statistics
  - Storage
  - ARP Table
  - Routes
  - Protocol Statistics
  - SNMP Statistics

- Services
  - Client Connections
  - Server Connections
Figure 2 shows a sample AdvantEDGE View CPU Statistics query. You can use this query to keep track of the total percentage of CPU that was in use for a query period and the percentage of time spent in idle, user, system, and wait (UNIX only) modes.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Idle Percent</th>
<th>User Percent</th>
<th>System Percent</th>
<th>Wait Percent</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sparc, 9,270 MHz</td>
<td>28 %</td>
<td>52 %</td>
<td>18 %</td>
<td>2 %</td>
<td>22 days, 4:52:36</td>
</tr>
<tr>
<td></td>
<td>System Average</td>
<td>28 %</td>
<td>52 %</td>
<td>18 %</td>
<td>2 %</td>
<td></td>
</tr>
</tbody>
</table>

![Graph showing CPU statistics](image)

**Figure 2. Sample AdvantEDGE View CPU Statistics Query**

For more information about AdvantEDGE View queries, refer to the *eHealth AdvantEDGE View User Guide* and the AdvantEDGE View Web Help. AdvantEDGE View also provides Application queries. For more information, refer to “Using AdvantEDGE View To Query eHealth AIMs for Application Data” on page 75.

**Viewing and Modifying SystemEDGE Configuration Information**

The SystemEDGE agent stores its configuration and monitoring information in the `sysedge.cf` and `sysedge.mon` configuration files. These files contain a series of configuration directives that describe the types of monitoring that the SystemEDGE agent will perform. The `sysedge.cf` file is static, but you can modify the `sysedge.mon` file through SNMP Sets. AdvantEDGE View provides a user interface for viewing and modifying the self-monitoring entries in the `sysedge.mon` file. Entries in `sysedge.cf` take precedence over entries in `sysedge.mon`. 
To display SystemEDGE configuration information:

1. Select a target system or group from the System or Group list of the AdvantEDGE View interface.

2. Select one of the following monitoring options from the Configuration list:
   - Self Monitoring (for monitoring thresholds)
   - Process Monitoring
   - Process Group Monitoring
   - Logfile Monitoring
   - NT Event Monitoring
   - History Collection

3. Click the Configuration icon.
   If you selected a system, AdvantEDGE View displays the self-monitoring table that matches the option that you selected. If you selected a group, AdvantEDGE View displays the Group Operations form. For more information about completing the form, refer to the AdvantEDGE View Web Help.

   After you display these tables, you can use AdvantEDGE View to modify them. For information about modifying the entries in the self-monitoring tables, refer to the eHealth AdvantEDGE View User Guide or Web Help.

Using eHealth To Collect and Report on System Data

This section explains how eHealth manages and monitors systems. You can use eHealth to troubleshoot or optimize the performance of your systems by focusing on the following types of information:

- Bandwidth utilization
- CPU utilization
- Memory utilization and paging
Discovering System Elements

Before you can run reports with eHealth, you must identify the system elements in your enterprise. You can either use the eHealth discover process to identify system elements, or you can import the system information using the DataSync database configuration information (DCI) import process.

When you run the eHealth discover process for System elements, eHealth searches the specified IP addresses for systems. When eHealth discovers a system, it creates a system element and the following:

- CPU element for each CPU in the system
- Disk element for each disk in the system
- Partition element for each partition, file system, or disk volume in the system
- Interface element for each interface on the system
- Process and process set elements for the processes that are defined on the system

**NOTE**

eHealth creates process elements and process set elements for a system if the system has a SystemEDGE agent and if the application that is running on that system is defined in the process definition file. For more information, refer to “Configuring System Process Sets” on page 53.

Using the Discover Process to Collect Data from System Elements. When you run the discover process and select System mode, eHealth searches the specified IP addresses for systems. You can specify an additional discover option for systems: Find Processes (Specify write community). By default, this option is selected when you select System mode.
When you discover systems with the **Find Processes (Specify write community)** option, you can track the impact of individual processes in the system. For more information, refer to “Configuring System Process Sets” on page 53.

**To discover system elements:**

1. On the eHealth console, select **Setup → Discover**. The Discover dialog box appears.

2. Select **System** under **Mode**.

3. Specify one or more community strings that allow read-write or read-only permission to the application elements in the **Community Strings** field.
4. Select the method through which you want to discover elements under Discover Using and specify the IP addresses to use, if necessary.

5. Complete any of the remaining fields in the Discover dialog box, if necessary; then click Discover. (For detailed instructions about running the Discover process, refer to the eHealth Administration Guide.)

Scheduling Data Collection for System Elements

After you identify the system elements, you need to collect performance data from them on a regular basis. You can create a scheduled job to collect data automatically through the eHealth poller, and you can import data using the DataSync database data information (DDI) tools. For more information about using DataSync, refer to the eHealth Integration Guide.

To schedule a discover job for system elements:

1. On the eHealth console, select Setup → Schedule Jobs. The Schedule Jobs dialog box appears.
2. Select Add Discover from the drop-down list box on the right side of the dialog box. The Add Scheduled Discover dialog box appears.
3. Select System under Mode.
4. Specify one or more community strings that allow read-write or read-only permission to the system elements in the Community Strings field.
5. Specify IP addresses in the IP Address List field.
6. Complete any of the remaining fields in the Add Scheduled Discover dialog box, if necessary; then click Schedule. (For detailed instructions about running the Discover process, refer to the eHealth Administration Guide.)
Viewing Unlicensed SystemEDGE Agents

When you discover system elements, eHealth discovers both licensed and unlicensed SystemEDGE agents. You can view unlicensed agents if you have licensed Fault Manager.

To view a list of the unlicensed agents:

1. On the eHealth console, select Setup → Poller Configuration. The Poller Configuration dialog box appears.

2. Select Unlicensed SysEdge Element in the List Elements of Type field, and click Refresh Element List. You can rediscover these elements after you license them through AdvantEDGE View. When they are licensed, eHealth can begin to poll them.

   For information about licensing the agents, refer to “Licensing SystemEDGE Agents and eHealth AIMs that eHealth discovered” on page 32.

Creating Groups and Group Lists for System Elements

Before you generate System reports, you might want to organize your system elements by creating groups and group lists.

Creating System Groups. Groups help you manage your elements. Create groups to organize system elements that are related in some way.

To create groups of application service elements:

1. On the eHealth Console, select Reports → Edit Groups → System Groups to display the System Groups dialog box.

2. Click Add. The Add System Groups dialog box appears.
3. Specify a name for the new application group in the **Group Name** field.
   You can specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). The word All and spaces are not permitted.

4. Optionally, reduce the number of elements shown in the **Available Elements** list by specifying a string in the **Filter by Name** field.

5. Select application elements from the **Available Elements** list that you want to add to the group.

6. Move the selected elements to the **Group Members** list by clicking the top arrow. To move a single element, select the element and either click the top arrow or double-click the element.

7. When you have completed the group, click **OK** or **Apply** to save the group. The new group appears in the Application Groups dialog box.

8. Click **Close** to save your groups and close the System Groups dialog box.

**Creating System Group Lists.** A **group list** is a collection of one or more groups. A group can belong to more than one group list. By creating group lists, you can associate groups that are related in some way.

**To create lists of system groups:**

1. On the eHealth console, select **Reports → Edit Group Lists → System Group Lists** to display the System Group List dialog box.

2. Click **Add**. The Add System Group List dialog box appears.

3. Specify a name in the **Group List Name** field using the criteria specified in step 3 on page 41.
4. Optionally, reduce the number of groups shown in the **Available Groups** list by specifying a string in the **Filter by Name** field.

5. Select the groups to add to the group list, as described in step 5 on page 41.

6. Move the selected groups to the **Group List Members** list by clicking the top arrow. To move a single group, select the group, and either click the top arrow or double-click the group.

7. Optionally, remove groups from the group list by selecting the groups in the **Group List Members** list and clicking the bottom arrow.

8. When you finish creating the system group lists, click **OK** or **Apply**. The new group list appears in the Group List dialog box.

9. Click **Close** to save your group lists and close the System Group List dialog box.

---

**eHealth Reports for Systems**

After you identify the system elements that you want to manage, you can use eHealth to generate the following types of reports for systems:

- At-a-Glance
- Trend
- Top N
- What-If Capacity Trend
- MyHealth

You can also purchase additional licenses to run the following types of eHealth reports:

- Health reports
- Service Level reports
eHealth reports provide you with details about the important performance indicators for systems. You can focus your management efforts by comparing systems to find those that are utilized most or those that have the most urgent problems.

eHealth reports for systems summarize the data from the network interfaces to determine the amount and type of traffic that passed through the system, but it does not report on individual network interfaces. To obtain reports on individual interfaces, use the eHealth — Network portion of the eHealth product suite. For more information, refer to the Network Health Administration Guide.

**NOTE**

You can create custom variables and then build custom reports on those variables if you have purchased the eHealth Custom Variable product and you have an eHealth — Report Developer license. For more information, refer to the eHealth Customizing Variables Guide and the eHealth Report Designer Guide.

To run eHealth reports:

1. Access the eHealth Web interface by starting your Web browser, and enter the IP address or hostname of the system on which you are running eHealth. For example, if you are running eHealth on the system named aview, enter the following:

   http://aview

   The eHealth Welcome page appears.

2. Enter your user name and password in the **User Name** and **Password** fields. The eHealth Web interface appears.

3. Click the **Run Reports** tab. The AdvantEDGE View page appears. The Run Reports page appears.

4. In the left pane, click the name of the report that you want to run.
5. Select System under Technology.

6. Complete the form, and click Generate Report.

The next sections provide general information about the reports that you can run with eHealth — System and Application. For detailed information, refer to the the eHealth Reports Guide and the eHealth Web Help.

**At-a-Glance Reports for Systems**

An At-a-Glance report for system elements provides summary capacity statistics for the specified system, including CPU, interface, and partition utilization; disk faults and I/O; and system availability. With these reports, you can quickly isolate busy CPUs or full disks and compare groups of systems. Figure 3 shows a sample At-a-Glance report for a system element.
Figure 3. Sample eHealth At-a-Glance Report for System Elements

eHealth — System and Application Administration Guide
Trend Reports for Systems

You can use Trend reports to see the value of one or more variables for your systems over a specified report period. This can help you to track the values of the variables to see when values might have changed radically or when a particular event, such as a reboot or missed poll, occurred.

Trend Variables

The Trend variables differ for each element type. You can run reports for the following types of systems and system components:

- CPU
- Disk
- Local Area Network (LAN)
- Process and Process Set
- User or System Partition
- Wide Area Network (WAN)

Each of these types includes specific variables on which you can run reports. For example, server disk elements have variables for disk reads and writes, storage capacity, and storage utilization. You can select up to ten variables at a time on which to run a Trend report. For a complete list of system Trend variables, refer to the eHealth Web Help.

Figure 4 shows a sample Trend report for the following variables:

- Total Bytes
- Total Incoming Bytes
- Total Outgoing Bytes
- System Calls
Figure 4. Sample Trend Report for Multiple System Variables
**Top N Reports for Systems**

A Top N report can list all elements in a group that exceed or fall below the report criteria goals that you specify. You can also specify the goal for each variable. eHealth calculates the difference between the actual value for that variable and the goal that you have set. Figure 5 shows a sample Top N report that lists the top seven system CPU elements that had an average CPU utilization above 80% during the report period.

<table>
<thead>
<tr>
<th>Element</th>
<th>CPU Utilization</th>
<th>Above 80</th>
<th>Goal 50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colorado-SH-Cpu</td>
<td></td>
<td>98.69</td>
<td>48.69</td>
</tr>
<tr>
<td>NewYork-SH-Cpu</td>
<td></td>
<td>94.34</td>
<td>44.34</td>
</tr>
<tr>
<td>Detroit-SH-Cpu-1</td>
<td></td>
<td>87.57</td>
<td>37.51</td>
</tr>
<tr>
<td>Boston-SH-Cpu-1</td>
<td></td>
<td>87.40</td>
<td>37.40</td>
</tr>
<tr>
<td>Atlanta-SH-Cpu</td>
<td></td>
<td>84.90</td>
<td>34.90</td>
</tr>
<tr>
<td>Houston-SH-Cpu-1</td>
<td></td>
<td>82.18</td>
<td>32.18</td>
</tr>
<tr>
<td>SanDiego-SH-Cpu-1</td>
<td></td>
<td>80.24</td>
<td>30.24</td>
</tr>
</tbody>
</table>

**Figure 5. Sample Top N Report for System CPU Utilization**

**What-If Capacity Trend Reports for Systems**

The eHealth What-If Capacity Trend report enables you to perform capacity planning by adjusting factors for capacity and demand until you have devised an appropriate what-if solution. By giving you the freedom to illustrate possible future scenarios, this report helps you prepare for problems before they occur.
MyHealth Reports for Systems

The MyHealth report page contains a series of charts that are tailored to a user’s particular interest. MyHealth provides eHealth Web users with one or more customized reports on the elements and groups that they consider critical. A MyHealth report page contains one or more panels, and each panel contains a separate chart.

Health Reports for Systems

You can run Health reports for your systems if you have a Health Reports license. A Health report contains information about the performance of a group of elements for a report period and alerts you to situations that require your attention. The report also identifies situations to investigate because of errors, unusual utilization rates, or excessive volume.

You can use a Health report to do the following:

- Identify normal and exceptional system behavior.
- Compare the performance of a group of elements during a report period to their performance over a baseline period.
- Detect changes in behavior that indicate that problems are about to happen or are currently happening.
- Identify trends in volume.
- Identify systems that require further investigation.
Health reports are generally several pages long. Figure 6 shows the Element Details page from a sample Health report for system elements.

Figure 6. Sample Element Details Page from a System Health Report
Service Level Reports for Systems

If you have a Service Level Reports license, you can run Service Level reports, which summarize the performance of your systems in four types of reports:

- **Executive**, which provides high-level views of the enterprise and can help you determine how workloads, availability, and latency vary with time across the enterprise and from group to group within the enterprise.

- **IT Manager**, which summarizes the service levels across an IT environment and provides information about the network volume, utilization, and Health exceptions, as well as a summary of important variables for each element in the group or group list.

- **Service Customer**, which provides information on volume, Health exceptions, utilization, Health Index, and availability for the systems in the group or group list.

- **Business Unit**, which summarizes the service level for the system resources that belong to a department, company, or organization.
Figure 7 shows a sample Executive Service Level report.

**eHealth Service Level Report**

**System**

**Executive Report**

Figure 7. Sample Executive Service Level Report for System Elements

*eHealth — System and Application Administration Guide*
If you are using eHealth — System and Application with the SystemEDGE agent, you can define and monitor process sets, which are collections of one or more processes that relate to a specific application. This chapter explains how to configure eHealth to create system process sets. It also explains how to troubleshoot potential problems with monitoring systems.

Configuring System Process Sets

If you have an eHealth — System license and the SystemEDGE agent is installed and licensed on your systems, you can use eHealth to report on the applications and processes that are running on those systems. This section describes how to use process sets to enable your system to monitor specific applications. You can also use eHealth — System and Application to monitor the performance of applications. For more information, refer to Chapter 4, “Managing and Monitoring Applications.”

Monitoring an Application's Effects on a System

It is important to monitor the effect of an application and its processes to determine whether a system can support the application effectively. If a system cannot support the application, users experience delays and problems while using the application.
Chapter 3  Configuring System Process Sets

Most systems track the impact of individual processes in the system. To monitor the impact of all processes that relate to an application, you must associate them with the application. eHealth uses a process definition to associate processes that you want to monitor as an application. It also identifies the process sets to discover. After polling the processes, eHealth then aggregates the data into the associated process set.

**NOTE**

To successfully monitor the processes, you must discover the system using a community string that has *read-write* permissions.

---

**Defining Process Sets**

If you have an eHealth license and the SystemEDGE agent, you can define process sets for the applications that are running on your systems to enable eHealth to find those processes during the discover process. After the discover process finishes, eHealth polls the SystemEDGE agent to obtain statistics on the discovered processes and creates elements for them in your poller configuration. After eHealth completes the discover process and successfully polls the process set data, you can generate reports to determine the impact of a process set on certain system variables, such as CPU utilization.

**Using Process Sets Effectively**

eHealth allows you to define various process sets to identify all processes that are running on your system and to monitor problems that occur with a particular application. As applications change or become obsolete, you should redefine, delete, or rename the process sets as necessary.
For example, you may want to define a process set to determine how your e-mail application’s processes affect the CPU utilization of your mail server and its clients. When you later upgrade your e-mail application to the next release, you can modify the process set definition to ensure that eHealth creates an element for the processes contained in the new release.

In addition, you can define a process set to monitor low-priority background processes specifically. These processes run in low-priority mode because they are not time-critical; therefore, they should not be allowed to consume system resources that are needed by higher priority processes. To ensure that eHealth does not include these processes in its calculation for total CPU utilization, you can configure process sets to ignore the impact of these processes.

**Using Discover Rules To Discover Process Sets**

eHealth uses discover rules when it attempts to discover a process set. It adds a particular set of eHealth elements to your poller configuration during the discover process based on the discover rule that you specify. When you create a new process set, eHealth uses a default discover rule named **Create Always**. The discover process creates elements for all processes that you include in the process definition for that process set, regardless of whether a given process is actually running.

You can accept the default discover rule, or you can do one of the following:

- **Select Create if Key Process is Found.** eHealth creates elements for the process set and all of its processes only if it finds the key process. The key process is a unique and persistent process for the application.

- **Select Create if Found.** eHealth creates elements for those processes that it finds. Discover finds a process only if it is actually running.

- **Select Create if Key Process and Found.** If eHealth finds the key process, it creates elements for the key process and only those processes that are running.
Reporting on Individual Process Elements in a Process Set

By default, eHealth does not store the polled statistics data for individual process elements in the database. To report on individual process elements, you must add the environment variable NH_STORE_PROCESS_DATA to your system before discovering those elements and set its value to yes. (The default value is no.) For instructions on setting this variable, refer to the eHealth Administration Reference.

**NOTE**

eHealth can poll process elements only for a system for which you have specified a community string that has read-write permissions.

Process sets do consume a poller license. To obtain a list of all elements in your poller configuration and to determine whether they require licenses, use the nhListElementLicenses command. For instructions about using nhListElementLicenses, refer to the eHealth Administration Reference.

Creating a Process Set for an Application

When you define the interactive discover process for your systems, you can also create one or more process sets for an application that runs on the system. Through the interactive discover process, you can identify process sets that you have defined previously.
To create a process set for an application:

1. Select **Setup → Discover** from the eHealth console. The Discover dialog box appears.

2. Select **System**, and ensure that **Find Processes (Specify write community)** is selected. It is selected by default.

3. Specify a community string that has read/write permissions in the **Community Strings** field.

4. Click **Define**. The Process Definition Editor dialog box appears.
5. Click **New** next to the **Process Set** list. The New Process Set dialog box appears.

6. Specify the name of the process set in the **Process Set Name** field.

7. Optionally, define the version of the application that you want to monitor by specifying a value in the **Process Set Version** field.
Define Process Sets

NOTE

The Process Set Version field is a descriptive field. eHealth does not validate your entry.

8. Click OK. The New Process Set dialog box closes. In the Process Definition Editor dialog box, eHealth highlights the new process set in the Process Set list and displays the name in the Process Set field, but it does not display any process names in the Name field below it.

9. Click New next to the process list. The New Process dialog box appears.

10. Specify the name of a process in the Process Name field. This name must be the actual string for which the discover process searches. You must specify it exactly as it appears in the system’s process list. You can view this information from an AdvantEDGE View Process Information query. For more information, refer to the AdvantEDGE View Web Help.
11. Specify the matching method that eHealth should use during the discover process. Do one of the following:

- Accept **Full Name** next to **Match** (the default). When eHealth detects a running process whose name *matches* the text that you specified in the **Process Name** field, it creates a process element.

- Select **Root Name**. When eHealth detects a running process whose root name contains the text that you specified in the **Process Name** field (excluding arguments), it creates a process element.

12. Optionally, specify a string in the **Arguments** field to uniquely identify this process. For example, if you were creating a process set to monitor your eHealth system, you could create a process named nhiPoller and specify the `-live` argument in its definition to instruct your system to monitor the Live Trend poller process.

**NOTE**

Use the **Arguments** field only if you have multiple processes that have the same name and use unique fixed arguments when they are run simultaneously.

13. Optionally, if the process is a unique and persistent process for the application, select **Key Process**. If eHealth finds this process during the discover process, it creates elements for all processes in the process set.

14. Optionally, if you do not want eHealth to include a process when determining a process set’s availability, deselect **Mandatory Process**.

15. Specify the operating system on which the process can run by selecting a name from the **Operating System** list.


17. Create more processes by repeating Steps 9 through 16.
18. Optionally, in the Process Definition Editor dialog box, exclude these processes from eHealth’s calculation for total CPU utilization by selecting **Exclude all processes from CPU utilization calculation**.

19. Accept the default discover rule, **Create Always**, or select another rule from the **Discover Rule** list. For information concerning the discover rules, refer to “Using Discover Rules To Discover Process Sets” on page 55.

20. Click **OK**. The Process Definition Editor dialog box closes and the Discover dialog box remains open.

21. Complete the remaining fields to define your interactive discover process; then run the discover process. For instructions, refer to “Using the Discover Process to Collect Data from System Elements” on page 37.

**Deleting Processes from a Process Set Definition**

You can delete a process from a process set. You can also remove all existing processes and add new processes to the set. To do so, you must delete the process set and recreate it. For instructions, refer to the next section, “Deleting a Process Set Definition.”

**To delete a process from the process set definition:**

1. Select **Setup → Discover** from the eHealth console. The Discover dialog box appears.

2. Select **System** and **Find Processes (Specify write community)**; then click **Define**. The Process Definition Editor dialog box appears.

3. Select a process set from the **Process Set** list; then select a process from the process list.

4. Click **Delete** to the right of the process list. The Confirm Delete dialog box appears.

5. Click **Yes**. The Confirm Delete dialog box closes and eHealth deletes the process from the process set’s definition.
6. To remove additional processes, repeat Steps 3 through 5 for each process that you want to remove.

7. Click **OK** in the Process Definition Editor dialog box to apply the changes. If you click **Cancel** instead of **OK**, eHealth displays a Confirm Cancel dialog box, requiring you to confirm that you want to cancel the change.

**Deleting a Process Set Definition**

If you no longer want to discover an application and its associated processes, you can delete the application’s process set from the process definition.

**To delete a process set:**

1. Select **Setup → Discover** from the eHealth console. The Discover dialog box appears.

2. Select **System** and **Find Processes (Specify write community)**; then click **Define**. The Process Definition Editor dialog box appears.

3. Select a process set from the **Process Set** list; then click **Delete** to the right of the **Process Set** list. The Confirm Delete dialog box appears.

4. Click **Yes**. eHealth removes the specified process set and its associated processes from the process set definition and closes the Confirm Delete dialog box.

5. In the Process Definition Editor dialog box, click **OK** to apply the changes. If you click **Cancel** instead of **OK**, eHealth displays a Confirm Cancel dialog box, requiring you to confirm that you want to cancel the change.
Example: Creating a Process Set

The following example demonstrates how to create a process set to monitor your eHealth system:

1. From the eHealth console, select **Setup → Discover**. The Discover dialog box appears.
2. Select **System** under **Mode**; then select **Find Processes (Specify write community)**.
3. Specify a community string in the **Community Strings** field that has read-write permissions.
4. Click **Define**. The Process Definition Editor dialog box appears.

5. Click **New** next to the **Process Set** list. The New Process Set dialog box appears.
6. Specify ehealth in the **Process Set Name** field.

7. Optionally, specify 5.6 in the **Process Set Version** field. This is the version of eHealth that you want to monitor.

   **NOTE**
   
   The **Process Set Version** field is a descriptive field.
   eHealth does not validate your entry.

8. Click **OK**. The New Process Set dialog box closes. In the Process Definition Editor dialog box, eHealth highlights the new process set in the **Process Set** list and displays the name in the **Process Set** field, but it does not display any process names in the **Name** field below it.

9. Click **New** next to the process list. The New Process dialog box appears.
10. Add the key process first by doing the following:
   a. Specify `nhiServer` in the **Process Name** field.
   b. Accept **Full Name** as the matching method (the default).
   c. Select **Key Process** to define this process as a unique and persistent process for this application.
   d. Accept **Mandatory Process** (the default) to include this process when determining this process set’s availability.
   e. Accept **any** from the **Operating System** list (the default).
   f. Click **OK**.
   g. In the Process Definition Editor dialog box, select **Create if Key Process is Found** from the **Discover Rule** list. eHealth will create elements for the nethealth process set and all of its processes only if it finds the nhiServer process.
   h. Click **New** next to the process list to display the New Process dialog box.

11. Add the second process by doing the following:
   a. Specify `nhiDbServer` in the **Process Name** field.
   b. Accept **Full Name** as the matching method (the default).
c. Accept **Mandatory Process** (the default) to include this process when determining this process set’s availability.

d. Accept **any** from the **Operating System** list (the default).

e. Click **OK**.

f. In the Process Definition Editor dialog box, select **New** next to the process list to display the New Process dialog box.

12. Add the third process by doing the following:

a. Specify **nhiConsole** in the **Process Name** field.

b. Accept **Full Name** as the matching method (the default).

c. Accept **Mandatory Process** (the default) to include this process when determining this process set’s availability.

d. Accept **any** from the **Operating System** list (the default).

e. Click **OK**.

f. In the Process Definition Editor dialog box, select **New** next to the process list to display the New Process dialog box.

13. Add the fourth process by doing the following:

a. Specify **nhiLiveExSvr** in the **Process Name** field.

b. Accept **Full Name** as the matching method (the default).

c. Accept **Mandatory Process** (the default) to include this process when determining this process set’s availability.

d. Select **any** from the **Operating System** list.

e. Click **OK**.

f. In the Process Definition Editor dialog box, select **New** next to the process list to display the New Process dialog box.

14. Add the fifth process by doing the following:

a. Specify **nhiPoller** in the **Process Name** field.

b. Accept **Full Name** as the matching method (the default).

c. Specify **-live** in the **Arguments** field. This argument instructs your system to monitor the Live Trend poller.

d. Accept **Mandatory Process** (the default) to include this process when determining this process set’s availability.
e. Accept any from the Operating System list (the default).
f. Click OK; then click OK in the Process Definition Editor dialog box.

Sample Reports for Process Sets

After you create process sets, you can use eHealth to run At-a-Glance, Trend, Top N, What-If, and MyHealth reports for your process sets. For example, you can run an At-a-Glance report for a System Process Set and use the CPU Utilization by Process Set chart to determine the CPU utilization for each process group that you have created. You can compare the utilization trends to see which process set consumed the most CPU processing resources over the report period.
When you click this chart, eHealth displays the All Process Sets – CPU Utilization by Process Set chart, which you can use to compare when and how much each process set utilizes the CPU resources of the system. This information can help you to determine whether a process set is overloading the CPU resources so that you can consider relocating applications to other systems to improve system and application performance. Figure 9 shows a sample All Process Sets – CPU Utilization by Process Set chart from a system At-a-Glance report.
Troubleshooting Systems

This section describes how to identify and troubleshoot problems when you are monitoring systems that use eHealth with the SystemEDGE agent.

Resolving Errors in Polling

To successfully monitor processes that are running on systems that use the SystemEDGE agent, you must use a community string that has read-write permissions to discover the systems. eHealth requires a community string with read-write access. If you detect errors when you are polling these discovered elements, you need to specify another community string.

To replace the community string for defined process sets:

1. Select Setup → Discover from the eHealth console. The Discover dialog box appears.
2. Select Systems and Find Processes (Specify write community).
3. Specify a community string that has read-write permissions in the Community Strings field.
4. Complete the remaining fields, if necessary.
5. Click Discover to start the discover process. For more information about running the discover process, refer to the eHealth Administration Guide.

Resolving Excessive Use of Disk Space by SystemEDGE Log Files

As eHealth polls the eHealth elements that support the SystemEDGE agent and eHealth AIMs, the SystemEDGE agent writes information and warning messages to the sysedge.log file (for Windows) or the syslog facility (on UNIX), by default. You may want to limit the size of these files to conserve disk space. For instructions on limiting the file size, refer to the section on configuring the SystemEDGE agent to use alternative syslog facilities in the eHealth SystemEDGE User Guide.
Managing and Monitoring Applications

With eHealth — System and Application, you can report on specific information about applications that are running on systems managed by SystemEDGE agents and eHealth AIMs. This chapter explains how to use eHealth to discover application elements and how to run eHealth application reports and AdvantEDGE View application queries to view the data that SystemEDGE and the eHealth AIMs collect.

Introduction

When you have an eHealth – Application Insight license, eHealth can collect and report on data from SystemEDGE agents that reside on systems where eHealth AIMs are also installed and licensed. If you have an AdvantEDGE View license, you can also query SystemEDGE agents and eHealth AIMs from the AdvantEDGE View page of the eHealth Web interface.

To monitor your applications most effectively, you must have the following components:

- eHealth (with Application Insight and AdvantEDGE View licenses)
- SystemEDGE agents (installed on every system that you want to monitor)
- eHealth AIMs (installed with the SystemEDGE agent on the systems that you want to monitor)
NOTE

Each system that is running applications you want to monitor requires only one SystemEDGE agent. You can install multiple eHealth AIMs on each system.

To specify license information for the first time, follow the instructions in the *eHealth Installation Guide: New Installations* for your platform. To modify license information, refer to the online help that is available from the eHealth console.

**Collecting Application Data**

Before you can collect application data, you must install and configure a SystemEDGE agent and an application-specific eHealth AIM on your system. You can then discover applications and add elements that represent the applications to the poller configuration.

**To collect data for application service elements:**

1. Install and configure the SystemEDGE agent on the system that you want to monitor. For instructions, refer to the *eHealth SystemEDGE User Guide*.
2. On the same system, install and configure the eHealth AIM for the application that you want to monitor. For instructions, refer to the user guide for the eHealth AIM that you are using.
3. From the eHealth console, discover application elements. For instructions, refer to “Using eHealth To Collect and Report on Application Data” on page 76.
4. Run reports on the discovered elements that provide application-specific data. For instructions, refer to “Creating Groups and Group Lists for Application Elements” on page 81.
When you have an Application Insight license, you can run eHealth reports on application service elements, as illustrated in Figure 10. Application service elements represent an application instance that is monitored by an eHealth SystemEDGE agent and an eHealth AIM.

![Diagram of eHealth System and Application Service Elements]

**Figure 10. Obtaining Application Data**

**Using the SystemEDGE Agent and eHealth AIMs To Collect Application Data**

As standalone components, SystemEDGE agents monitor the systems on which they are installed. When you install an application-specific eHealth AIM on a system with a SystemEDGE agent, the agent can monitor the application that is running on the system, as well. The Application Insight license enables eHealth to discover applications that the agent and eHealth AIM are monitoring. eHealth receives the data that the SystemEDGE agent collects and stores it in the database for reporting.

The *eHealth SystemEDGE User Guide* explains how to install, configure, and use the agent. You must install and configure a SystemEDGE agent on each system that you want to monitor.
eHealth AIMS enable you to detect application performance problems, ensure that there are sufficient system resources for the applications that you are running, and track usage statistics for the applications. Using the eHealth AIMS, you can also monitor the effect of applications on critical system resources, and you can determine application configuration information.

Table 2 lists the existing eHealth AIMS and the applications for which they provide management.

<table>
<thead>
<tr>
<th>Module</th>
<th>Manages and Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth AIM for Apache</td>
<td>Apache Web server</td>
</tr>
<tr>
<td>eHealth AIM for Check Point FireWall-1</td>
<td>Check Point FireWall-1 application</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft Exchange</td>
<td>All key Microsoft Exchange services, such as the Connectors, Information Store, Exchange Directory, Message Transfer Agent, and more</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft IIS</td>
<td>Microsoft IIS Web server and its services, including World Wide Web (WWW), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP).</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft SQL Server</td>
<td>Microsoft SQL Server databases, including SQL core processes, queries, transaction logs, and backups.</td>
</tr>
</tbody>
</table>
Table 2. eHealth AIMs (Page 2 of 2)

<table>
<thead>
<tr>
<th>Module</th>
<th>Manages and Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth AIM for Network Services for UNIX</td>
<td>Vital network services for UNIX systems, including Sendmail, DNS, LDAP, NFS, NIS, and DHCP</td>
</tr>
<tr>
<td>eHealth AIM for Network Services for Windows</td>
<td>Vital network services for Windows systems, including Active Directory, DHCP, DNS, and WINS.</td>
</tr>
<tr>
<td>eHealth AIM for Oracle</td>
<td>Oracle database and application, including configuration information and status of Oracle processes and files.</td>
</tr>
</tbody>
</table>

For more information about these eHealth AIMs, refer to the user guide for the eHealth AIM that you want to use.

**Using AdvantEDGE View To Query eHealth AIMs for Application Data**

You can use AdvantEDGE View to view Application queries for each of the applications that can be monitored by the eHealth AIMs. You can query systems on which the SystemEDGE agent and the appropriate eHealth AIM are installed and licensed.

**To run an AdvantEDGE View Application query:**

1. Select the target system or group from the System or Group list.
2. Select the application that you want to monitor from the Applications list.
3. Click the **Applications** icon.

AdvantEDGE View runs the query for the specified application on the system or group you selected. For more information, refer to the *eHealth AdvantEDGE View User Guide* or the AdvantEDGE View Web Help.

Figure 11 shows a sample AdvantEDGE View query for the Microsoft Exchange application’s disk usage.

![Figure 11. Microsoft Exchange Disk Usage](image)

Using **eHealth** To Collect and Report on Application Data

After you configure the SystemEDGE agent and eHealth AIMs to collect application data, you can use eHealth to discover applications and to report on them.

**Discovering Application Elements**

Using the eHealth discover process, you can discover application elements and automatically add them to the poller configuration. When you run the discover process and select the **Application** mode (as described in “To discover application elements:” on page 77), eHealth searches the list of IP addresses for applications. It finds an application when it locates a system that is running both the SystemEDGE agent and an eHealth AIM. When you discover an application, eHealth creates an application service element and an application service process set element.
eHealth looks for application elements on User Datagram Protocol (UDP) port 1691 by default. You can configure eHealth to search for application elements on other agent ports by modifying the NH_DISCOVER_APPLICATION_PORTS environment variable. For more information on specifying ports, refer to the section on configuring the discover process to search for different ports in the eHealth Administration Guide. For instructions on setting environment variables, refer to the section on modifying environment variables in the eHealth Administration Reference.

To discover application elements:

1. On the eHealth console, select **Setup → Discover**. The Discover dialog box appears.

2. Select **Application** and **System** under **Mode**.
NOTE
If you do not select both System and Application modes, you cannot discover eHealth AIMS.

3. Specify one or more community strings that allow read-write or read-only permission to the application elements in the Community Strings field.

4. Select the method through which you want to discover elements under Discover Using and specify the IP addresses to use, if necessary.

5. Complete any of the remaining fields in the Discover dialog box, if necessary; then click Discover. (For detailed instructions for running the Discover process, refer to the eHealth Administration Guide.)

Viewing Unlicensed eHealth AIMS
When you discover application elements, eHealth discovers both licensed and unlicensed eHealth AIMS. You can view unlicensed eHealth AIMS if you have licensed Fault Manager.

To view the unlicensed eHealth AIMS:

1. On the eHealth console, select Setup → Poller Configuration. The Poller Configuration dialog box appears. The unlicensed eHealth AIMS have a suffix of unlicensed.

2. To view only the unlicensed SystemEDGE agents, eHealth AIMS, and Service Availability modules, select Unlicensed SysEdge Element in the List Elements of Type field, and click Refresh Element List. You can rediscover these elements after you license them through AdvantEDGE View or Live Health. When they are licensed, eHealth can begin to poll them.

For information about licensing the agents, refer to “Licensing SystemEDGE Agents and eHealth AIMS that eHealth discovered” on page 32.
Scheduling Data Collection for Application Elements

After you identify the application elements, you need to collect performance data from them on a regular basis. You can create a scheduled job to collect data automatically through the eHealth poller, and you can import data using the DataSync database data information (DDI) tools. For more information about using DataSync, refer to the eHealth Integration Guide.

To schedule a discover job for application elements:

1. On the eHealth console, select **Setup → Schedule Jobs**. The Schedule Jobs dialog box appears.
2. Select **Add Discover** from the drop-down list box on the right side of the dialog box. The Add Scheduled Discover dialog box appears.
3. Select **Application** and **System** under **Mode**.
4. Specify one or more community strings that allow read-write or read-only permission to the application elements in the **Community Strings** field.
5. Specify IP addresses in the **IP Address List** field.
6. Complete any of the remaining fields in the Add Scheduled Discover dialog box, if necessary; then click **Schedule**.

For a description of the other discover options, refer to the section on defining the discover process in the eHealth Administration Guide.

Application Element Naming Conventions

When you discover application elements, eHealth names the elements using the format defined in Table 3. eHealth creates application service elements to represent monitored applications that reside on a system that the SystemEDGE agent
is monitoring. eHealth also creates application service process sets that monitor the footprint information of each application service. eHealth creates a unique element name for each element, as defined in Table 3.

Table 3. Application Element Name Formats

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application service</td>
<td><code>hostname-AH-moduleName</code></td>
</tr>
<tr>
<td>Application service process sets</td>
<td><code>hostname-AH-moduleName-ProcessSet</code></td>
</tr>
</tbody>
</table>

**Deleting Application Elements**

You can delete application elements using the Poller Configuration dialog box. To access this dialog box, select **Setup → Poller Configuration** on the console.

To delete one or more application elements, do one of the following:

- Select a single row in the **Element Name** list, and then click **Delete**.
- Select multiple, continuous rows by clicking on the first element in the section to delete, press and hold the **Shift** key, click the last row of the section, and then click **Delete**.
- Select multiple, non-continuous rows to delete by holding the **Ctrl** key while clicking on the various rows, and then click **Delete**.

If you delete an application service element, you also delete all process sets that are associated with that element.

**CAUTION**

You must click **OK** or **Apply** in the Poller Configuration dialog box to save your changes. If you click **Cancel**, you will lose all work that you have performed since you opened the Poller Configuration dialog box.
Creating Groups and Group Lists for Application Elements

Before you generate Application reports, you might want to organize your application service elements by creating groups and group lists.

Creating Application Groups. Groups help you manage your elements. Create groups to organize application elements that are related in some way.

To create groups of application service elements:

1. On the eHealth Console, select Reports → Edit Groups → Application Groups to display the Application Groups dialog box.
2. Click Add. The Add Application Groups dialog box appears.
3. Specify a name for the new application group in the Group Name field. You can specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). The word All and spaces are not permitted.
4. Optionally, reduce the number of elements shown in the Available Elements list by specifying a string in the Filter by Name field.
5. Select application elements from the Available Elements list that you want to add to the group using any of the following methods:
   • Select the first element and hold down the mouse button while you select adjacent elements.
   • Select the first element that begins a range, scroll through the list, press Shift, and select the element that ends the range.
   • Select non-adjacent elements by pressing Ctrl while selecting elements, and optionally, deselect elements by pressing Ctrl and clicking the elements.
6. Move the selected elements to the Group Members list by clicking the top arrow. To move a single element, select the element and either click the top arrow or double-click the element.

7. When you have completed the group, click OK or Apply to save the group. The new group appears in the Application Groups dialog box.

8. Click Close to save your groups and close the Application Groups dialog box.

Creating Application Group Lists. A group list is a collection of one or more groups. A group can belong to more than one group list. By creating group lists, you can associate groups that are related in some way.

To create lists of application groups:

1. On the eHealth console, select Reports → Edit Group Lists → Application Group Lists to display the Application Group List dialog box.

2. Click Add. The Add Application Group List dialog box appears.

3. Specify a name in the Group List Name field using the criteria specified in step 3 on page 81.

4. Optionally, reduce the number of groups shown in the Available Groups list by specifying a string in the Filter by Name field.

5. Select the groups to add to the group list, as described in step 5 on page 81.

6. Move the selected groups to the Group List Members list by clicking the top arrow. To move a single group, select the group, and either click the top arrow or double-click the group.

7. Optionally, remove groups from the group list by selecting the groups in the Group List Members list and clicking the bottom arrow.
8. When you finish creating the application group lists, click **OK** or **Apply**. The new group list appears in the Group List dialog box.

9. Click **Close** to save your group lists and close the Application Group List dialog box.

**eHealth Reports for Applications**

With eHealth and an Application Insight license, you can run At-a-Glance, Trend, and Top N reports for application service elements. You can also customize these reports. For more information, refer to the chapters on generating and customizing reports in the *eHealth Administration Guide*.

**NOTE**

You can create custom variables to monitor your applications and then build custom reports for those variables if you have purchased the eHealth Custom Variable product and you have an eHealth — Report Developer license. For more information, refer to the *eHealth Customizing Variables Guide* and the *eHealth Report Designer Guide*.

**To run eHealth reports:**

1. Access the eHealth Web interface by starting your Web browser, and enter the IP address or hostname of the system on which you are running eHealth. For example, if you are running eHealth on the system named aview, enter the following:

   **http://aview**

   The eHealth Welcome page appears.

2. Enter your user name and password in the **User Name** and **Password** fields. The eHealth Web interface appears.

3. Click the **Run Reports** tab. The Run Reports page appears.
4. In the left pane, click the name of the report that you want to run.

5. Select **App Service** under **Technology**.

6. Complete the form, and click **Generate Report**.

For more information about eHealth reports, refer to the eHealth Reports Guide and the eHealth Web Help.

**At-a-Glance Reports for Applications**

You can use an At-a-Glance report to show the performance of an application service element during the report period. The Application Service At-a-Glance report charts show trends for important application performance variables.

If you also discovered the systems using **System** mode, you can monitor the health and performance of the system and its resources using System At-a-Glance reports in addition to the Application Service At-a-Glance reports. For more information, refer to “At-a-Glance Reports for Systems” on page 44.

When you run an At-a-Glance report for a specific application service that was monitored by an eHealth AIM, the report includes both footprint (if available) and application statistics for that application. Because the At-A-Glance reports for application service elements already contain information about the footprint variables, you will not be able to run these reports for the application process set elements. To obtain data for the application process set elements alone, you must run a Trend report.

At-a-Glance reports for applications include charts for variables that are specific to the application service you are monitoring. For example, if you are running an At-a-Glance report for Apache application service elements, it will include the Number of Apache Processes chart, as shown in Figure 12.
If you are running an At-a-Glance report for Oracle application service elements, it will include a Block Changes per Transaction chart, as shown in Figure 13.

Figure 13. Block Changes Per Transaction Chart from an At-a-Glance Report for Oracle Application Service Elements

If you are running an At-a-Glance report for Exchange application service elements, it will include a Disk Usage chart, as shown in Figure 14.
Trend Reports for Applications

You can use a Trend report to analyze the performance of an application service element or group of application service elements based on specific variables. You can run Trend reports on application process set elements for an application that was monitored by an eHealth AIM. The trend variables vary by application service, offering data that is very specific to the application you are monitoring. For example, for IIS application service elements, you can report on variables such as cache hit rate, disk usage, FTP bytes processed, WWW bytes processed, and so on. For SQL Server application service elements, you can report on very different variables, including average lock wait time, CPU utilization, disk space utilization, lock requests, and transactions. For more information, refer to the eHealth Web Help.

Top N Reports for Applications

You can generate a Top N report to list all application service elements in a group, or to list the elements in a group that exceed or fall below the report criteria goals that you specify.
MyHealth Reports for Applications

You can include charts for application service monitoring in your MyHealth reports. MyHealth provides eHealth Web users with one or more customized reports on the elements and groups that they consider critical. You can run MyHealth reports from the MyHealth tab in the eHealth Web interface.
Using Live Health with eHealth — System and Application

Live Health consists of the following applications:

- Live Exceptions
- Live Status®
- Live Trend

You can use these applications with eHealth and the SystemEDGE agent to obtain real-time information and alarm data for your elements.

Using Live Health with the SystemEDGE Agent

If you have a Live Health license and you are using eHealth — System and Application, you can configure the SystemEDGE agent to send traps to your eHealth system so that you can view SystemEDGE traps in the Live Exceptions Browser and manage them with Fault Manager.

Live Exceptions provides network operations center (NOC) and systems, application, and network management personnel with real-time alarms condition reporting by identifying problems that include delay, errors, failures, security, or configuration changes. It can display information about alarms in the Live Exceptions Browser, as well as send traps (alarms) to NMSs and other trap destinations.
Live Exceptions includes default profiles for all eHealth technology types. The profiles organize alarm variables by delay, availability, unusual workload, and latency. As a Live Health administrator, you can define alarm conditions by specifying variables to examine, thresholds to detect, and intervals over which to examine the data. You can also clear alarms manually and disable rules within a profile.

**Fault Manager**

*eHealth* Live Health — Fault Manager is an enhancement to Live Exceptions that enables *eHealth* to receive SNMP trap messages from devices and systems and to take actions based on Live Exceptions alarm rules. Fault Manager can receive traps from any device, such as the SystemEDGE agent, or any NMS, such as HP OpenView.

Fault Manager interprets and processes trap information. It reduces the noise of duplicate and repeated messages and alerts you to the problems and conditions that interest you. When the *eHealth* system receives a trap, it processes the trap based on Live Exceptions rules and profiles that you configure. Thus, you can configure Fault Manager to raise an alarm for the associated element, or to ignore various trap messages.

**NOTE**

You can edit the syssedge.cf file to configure the SystemEDGE agent to feed specific traps to Fault Manager for your systems and applications. For information about configuring SystemEDGE, refer to the *eHealth SystemEDGE User Guide*. For more information about using Fault Manager, refer to the *eHealth Live Health User Guide*. 

*eHealth — System and Application Administration Guide*
**TrapEXPLODER**

eHealth TrapEXPLODER is integrated with the Fault Manager software. It works as a trap pre-server, signaling and forwarding SNMP traps. When a connection is down, it buffers the data while trying to reestablish the connection. When the connection is reestablished, it forwards the buffered data.

**Using SystemEDGE Configuration Templates to Send Traps**

With AdvantEDGE View, you can create and manage SystemEDGE configuration templates. Each template can include entries for any or all of the SystemEDGE self-monitoring tables. AdvantEDGE View includes several default templates for monitoring specific types of systems (for example, all Solaris systems, all Windows systems, and so on), and you can create your own custom templates for configuring the SystemEDGE agent to send traps when certain events occur. For more information about using AdvantEDGE View to manage SystemEDGE configuration templates, refer to the *eHealth AdvantEDGE View User Guide*.

**Creating Groups of Systems**

Live Exceptions and Live Status monitor elements and display alarm information based on groups and group lists. An eHealth administrator must create groups and group lists through the eHealth console. You can create groups of systems that are being monitored by the SystemEDGE agent and by application-specific eHealth AIMS. For more information about using the console to create and maintain groups and group lists, refer to the *eHealth Administration Guide*.
Using the Live Exceptions Browser To View SystemEDGE Data

Live Exceptions includes a number of default profiles for SystemEDGE agents and eHealth AIMs. A profile is a set of one or more alarm rules that the Live Health administrator applies to a subject to monitor. Alarm rules define the type of element and conditions to monitor, thresholds and time duration, and the problem’s severity. Live Exceptions applies each rule in the profile to each element in the group or group list that matches the element type of the rule. After an administrator associates profiles with groups (or group lists), Live Exceptions begins to monitor the polled data from the specified elements and generates alarms accordingly. This data can be polled from SystemEDGE agents and eHealth AIMs. Live Exceptions matches such data against the default profiles for SystemEDGE and the eHealth AIMs and generates alarms as necessary. For information about modifying profiles or creating new ones, refer to the eHealth Live Health Administration Guide.

To view SystemEDGE data in the Live Exceptions Browser:

1. Do one of the following:
   - On Windows, select Start → Programs → eHealth 5.6 → Live Exceptions.
   - On UNIX, change to the /client/bin subdirectory of the Live Health installation, and enter nhLiveExceptions.

   The Login dialog box appears.

2. Enter the name of the system to which you want to connect in the eHealth System field, and then enter your user name and password in the Web User and Password fields. The Live Exceptions Browser appears.

3. In the Organization (left) Pane, select System and any groups you have defined, if desired. Live Exceptions displays the alarms for the groups you selected in the Event Table.
NOTE

If your eHealth system has Fault Manager, the Live Exceptions Browser displays event alarms. In addition, the Live Exceptions Browser contains additional information, including a technology type in the Organization Pane called Event Source and additional columns in the Event Table called Component, Event Carrier, Description, and Trap Count.

4. Select and right-click an alarm of interest. A drill-down menu appears.
5. Select any option to obtain more information about the element you selected, as follows:
   
   **a.** Select **At-a-Glance Report** to drill down to an At-a-Glance report for any element.
   
   **b.** If the element has an alarm based on a variable, select **Trend Report** to drill down to a Trend Report, or **Live Trend** to drill down to a Live Trend chart. You cannot drill down to a Trend report or Live Trend chart if the alarm is an event alarm.
   
   **c.** If the eHealth system for an element has a SystemEDGE agent and an AdvantEDGE View license, select one of the following options to drill down to one of the following AdvantEDGE View queries:
   
   - Select **System Information** to obtain high-level information about a system, including system name and location; operating system; version of the SystemEDGE agent; basic system resources; and the number of users, open files, and processes.
   
   - Select **Performance Information** to obtain overall performance statistics, including memory and swap capacity, I/O buffer and cache, system-wide CPU averages, and system load averages.
   
   - Select **Event Information** (only available for event alarms if the eHealth system has Fault Manager) to obtain event information, including the complete trap contents.
d. If the eHealth system for an element has an Application Response agent and an eHealth — Response license, select **Response Transaction Log** to drill down to the Agent Transaction Viewer.

e. Select **Reports** to drill down to the available reports for the element.

Using Live Status with SystemEDGE

Live Status provides a high-level view of the current status of your critical resources. It displays a diagram of the elements in a group list. Icons that represent the elements are color-coded to reflect their alarm and monitoring status. You can look at the display and quickly assess the state of your resources and identify trouble spots based on color changes in a logically grouped graph. You can also drill down from an element for details to understand the nature of the problem.

Before you can use Live Status, the eHealth administrator must define eHealth groups and group lists, and the Live Health administrator must use Live Exceptions to define and apply rules and profiles. For more information about creating groups and group lists, refer to the **eHealth Administration Guide**. For more information about defining rules and profiles, refer to the **eHealth Live Health Administration Guide**.

To start Live Status:

1. Do one of the following:
   - On Windows, select **Start → Programs → eHealth 5.6 → Live Status**.
   - On UNIX, change to the /client/bin subdirectory of the Live Health installation, and enter **nhLiveStatus**.

The Login dialog box appears.

2. Enter the name of the system to which you want to connect in the **eHealth System** field, and then enter your user name and password in the **Web User** and **Password** fields. The Open Diagram dialog box appears.
All existing Live Status diagrams that you have created appear under **Title**. The group list associated with the diagram appears under **Group List**.

3. Select the title of a Live Status diagram and click **OK**. The Live Status window displays the diagram you selected.

**NOTE**

You can display more than one Live Status window to monitor several critical group lists, and you can change the diagram to view a different group list. You can also save your favorite or most frequently used diagrams to open them at any time. For more information, refer to the **eHealth Live Health User Guide**.

Figure 15 shows a Live Status diagram for systems that the SystemEDGE agent is monitoring.

Figure 15. Live Status Diagram
You can right-click an element, group, or group list in the Live Status diagram to display a menu through which you can obtain more information.

**Drilling Down from a Group or Group List**

When you right-click on a group or group list, you can select one of the following options:

- Select **Live Exceptions** to display the Live Exceptions Browser, filtered to that group or group list.
- Select **Reports** to view a Web page that contains a list of existing reports run for that group or group list. If your account has permission, you can also run other reports.

**Drilling Down from an Element**

Depending on the type of element, your account permissions, the licenses on the eHealth system, and whether the alarm is an event or non-event alarm, you can drill down from an element to the following:

- Alarm Occurrences window in Live Exceptions
- Live Trend
- At-a-Glance report
- Trend report
- Reports list
- AdvantEDGE View
- Response Transaction Log for elements with Application Response agents

**Drilling Down to the Live Exceptions Alarm Occurrences Window.** If an element has an alarm, you can select the element and right click to drill down to a modified version of the Alarm Occurrences windows in Live Exceptions. The window appears with all alarms—including event alarms if the eHealth system has Fault Manager—for that element. If an element is a parent, the window contains alarms for its children (subcomponents) also.
NOTE

For information about the other drill-down options, refer to Step 5 in “To view SystemEDGE data in the Live Exceptions Browser:” on page 92.

Using Live Trend with SystemEDGE

If you have correctly configured Live Trend, you can drill down from AdvantEDGE View queries to Live Trend charts.

You can use Live Trend to create charts that monitor statistics elements that you are polling using eHealth. You can create a single chart or multiple charts in various styles to represent element trends (a single element with multiple variables) or variable trends (a single variable for multiple elements). Figure 16 shows a Live Trend chart for four variables on a system called atlanta.

![Figure 16. Live Trend Multi-Variable Chart](image)

*Figure 16. Live Trend Multi-Variable Chart*
To start Live Trend:

1. Do one of the following:
   - On Windows, select Start → Programs → eHealth 5.6 → Live Trend.
   - On UNIX, change to the /client/bin subdirectory of the Live Health installation, and enter nhLiveTrend.

   The Login dialog box appears.

2. Enter the name of the system to which you want to connect in the eHealth System field, and then enter your user name and password in the Web User and Password fields. The Live Trend Chart Definition Manager appears.

   You can create your own charts through the Live Trend Chart Definition Editor to specify the elements and variables for which you want to view data. For more information, refer to the eHealth Live Health User Guide and the Live Trend Help.

Viewing a Live Trend Chart

To view an existing Live Trend chart, select a chart definition from the Live Trend Chart Definition Manager dialog box and click Start. The Live Trend Chart Display dialog box displays the chart in the format in which it was last viewed and saved. You can modify the chart you are viewing using the View Menu.
Index

A
actions 26
adding custom MIB objects 26
AdvantEDGE View
administration 28
application queries 75
configuration information 29
deploying agents and eHealth AIMs 30
drilling down from Live Exceptions 94
handling traps and events 32
introduction 16
licensing agents and eHealth AIMs 32
preferences 29
querying SystemEDGE agents 33
templates for configuring SystemEDGE
and eHealth AIMs 30
viewing SystemEDGE configuration
information 35
Alarm Occurrences window 97
application
definition 12
monitoring effects on systems 12, 53
queries in AdvantEDGE View 75
reports
At-a-Glance 84
MyHealth 87
overview 83
running 83
Top N 86
Trend 86
Application Insight
collecting data 73
license 71
Application Response agents. See AR agents.
application service
discovering elements 76
elements 79
process sets 76, 80
applying SystemEDGE configuration
templates 31
AR agents, deploying 30
asset tracking 25
At-a-Glance reports
applications 84
drilling down from Live Exceptions 94
systems 44
Index

C
capacity planning 17
collecting data
  application 72
  historical 25
  system 37
creating
group lists
  applications 82
  systems 40
  groups
  applications 81
  systems 40
  process sets 56

D
defining process sets 54
deleting
  process from process set definition 61
  process set definition 62
deploying agents and eHealth AIMs 30
discovering
  application elements 76
  process sets 55
  system elements 37

E
eHealth
eHealth application reports
  At-a-Glance 84
  MyHealth 87
  Top N 86
  Trend 86
  overview 17
  poller 17
reports
  applications 83
  drilling down from
    Live Exceptions 95
  overview 18
  systems 43
system reports
  At-a-Glance 44
  MyHealth 49
  Top N 48
  Trend 46
  What-If Capacity Trend 48
using with SystemEDGE 53
eHealth — Network 19
eHealth — Response 19
eHealth — System and Application
  AdvantEDGE View 16
  components 12
eHealth 17
eHealth AIMs 15
  managing
    applications 14
    systems 13
  overview 14
  SystemEDGE agent 15
eHealth AdvantEDGE View.
  See AdvantEDGE View.
eHealth AIMs
  applications monitored 74
  collecting application data 73
  overview 15
  querying 75
eHealth application insight modules.
  See eHealth AIMs.
eHealth Live Health. See Live Health.
eHealth Service Availability 19
eHealth SystemEDGE. See SystemEDGE agent.
elements, discovering
application 77
system 37
extensions 26

F
Fault Manager
Live Exceptions Browser 93
overview 90

G
generating
AdvantEDGE View queries 33
reports
applications 83
systems 43
group lists, creating
applications 82
systems 41
groups, creating
applications 81
systems 40

H
Health reports
example 50
overview 49
history
collection 25
sampling 22

L
licensing SystemEDGE agents and
eHealth AIMs 32
Live Exceptions
drill-downs
AdvantEDGE View 94
At-a-Glance reports 94
eHealth reports 95
Live Trend 94
Response Transaction Log 95
Trend reports 94
drilling to reports 94
overview 92
profile 92
viewing alarms 92
Live Health
applications 89
Fault Manager 90
overview 18
system groups 91
using with SystemEDGE 89
Live Status
drilling down to
Alarm Occurrences window 97
eHealth reports 97
Live Exceptions Browser 97
overview 95
starting 95
Live Trend
drilling from Live Exceptions 94
overview 98
starting 99
viewing charts 99
log file monitoring 24
M
managing
  applications 14
  systems 13
MyHealth reports
  applications 87
  systems 49

N
name formats for application elements 80
NH_DISCOVER_APPLICATION_PORTS environment variable 77

P
perfmon extensions 26
poller 17
preferences in AdvantEDGE View 29
process
  definition file 13, 54
  elements 56
  monitoring 24
process group monitoring 24
process sets
  creating for an application 56
  defining 54
  deleting processes 61
  discover rules, using 55
  discovering 55
  example 63
  reporting on individual elements 56
  using effectively 54
Professional Services, contacting 9

Q
querying
eHealth AIs 75
SystemEDGE agents 33

R
reports
  At-a-Glance
    applications 84
    system 44
  drilling down from Live Exceptions to eHealth 95
  generating
    applications 83
    systems 43
    Health 49
    MyHealth
      applications 87
      systems 49
  running
    applications 83
    systems 43
  Service Level 51
  Top N
    applications 86
    systems 48
  Trend
    applications 86
    systems 46
  What-If Capacity Trend 48
  Response Transaction Log 95
S
scheduling discovery
  application elements 79
  system elements 39
self monitoring 23
Service Level reports 51
system
  creating process set elements 37
  definition 12
  identifying elements 37
process
  creating elements 37
  definition file 13, 54
  deleting 61
process set definition
  deleting 62
  modifying 61
process sets
  defining 54
  discovering 55
  example 63
reports
  At-a-Glance 44
  Health 49
  MyHealth 49
  overview 42
  running 43
  Service Level 51
  Top N 48
  Trend 46
  What-If Capacity Trend 48
SystemEDGE agent
  actions 26
  configuration templates
    applying 30
    creating 30
    traps 91
  custom MIB objects 26
history collection 25
log file monitoring 24
overview 15
process group monitoring 24
process monitoring 24
querying 33
self-monitoring features 23
service monitoring 24
templates
  applying 30
  configuring traps 91
  creating 30
  threshold monitoring 23
  viewing self-monitoring tables 35
Windows
  event monitoring 24
  extensions 26

T
Technical Support, contacting 9
templates for SystemEDGE
  applying 31
  configuring traps 91
  creating 30
  threshold monitoring 23
Top N reports
  applications 86
  systems 48
Top Processes 25
tracking assets 25
TrapEXPLODER 91
traps, handling
  AdvantEDGE View 32
  Fault Manager 90
trend
  analysis 17
  variables for systems 46
Trend reports
  applications 86
  drilling from Live Exceptions 94
  systems 46
troubleshooting problems with system
  monitoring 69

V
viewing
  alarms in Live Exceptions Browser 92
SystemEDGE agent
  configuration information 35
  data in Live Exceptions Browser 92
  self-monitoring tables 35
  traps in AdvantEDGE View 32
unlicensed
  eHealth AIMS 78
  SystemEDGE agents 40

W
What-If Capacity Trend reports 48
Windows
  event monitoring 24
  registry extensions 26