Administration Guide

r6.1
This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2008 CA. All rights reserved.
# Contents

## Chapter 1: Overview
- About This Guide .......................................................... 5
- Audience ........................................................................... 5
- Contact Technical Support ............................................. 5

## Chapter 2: About eHealth Response
- What is eHealth Response .................................................. 7
  - Application Response ...................................................... 8
  - Service Availability (SA) and Voice Quality Monitor (VQM) ...................................................................... 9
  - Cisco IOS IP Service Level Agreements (SLAs) ......................................................................................... 9
  - Juniper Real-Time Performance Monitoring (RPM) ................................................................. 10
- How eHealth Monitors Response Time .................................. 10
  - Response Endpoints and Paths .......................................... 11
  - Creating Response Paths .................................................. 11

## Chapter 3: Configure Application Performance Using Application Response
- How Application Response Monitors Application Performance .................................................. 13
  - Understand the Role of the AR Controller .................................................. 14
  - Monitor Applications with Application Response .................................................. 14
  - How AR Agents Measure Application Performance .................................................. 16
- Prepare for AR Agent Configuration ............................................ 17
  - License Application Response and AR Agents .................................................. 17
- Install, Configure, and Deploy AR Agents .............................................. 18
  - Get Started ........................................................................ 18
  - Plan Your Time .................................................................. 18
  - The Configuration Process .................................................. 19
- Upgrade AR Agents and Modify Advanced Settings .................................................. 23
  - Advanced Settings Page ...................................................... 23
- Uninstall AR Agents ................................................................. 26

## Chapter 4: Add Response Elements Using eHealth Response
- Overview of the Discover Process ............................................ 27
- Create Response Destination Elements ............................................ 28
- Create Response Paths ............................................................... 30
  - Response Element Naming Conventions .............................................. 32
- Verify That Your Application Response Paths Appear in eHealth .................................................. 33
  - Interpret Polling Errors on Response Path Elements .................................................. 33

## Chapter 5: Manage Response Elements Using eHealth Response
- Manage Response Path Elements ............................................. 35
- Modify Response Path Elements .................................................. 37
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Source and Destination Elements</td>
</tr>
<tr>
<td>Delete Response Elements</td>
</tr>
</tbody>
</table>

**Chapter 6: Manage Response Using eHealth Reports**

- Overview of Response Reports | 43
- Prepare to Run Response Reports | 45
  - Response Groups and Group Lists | 46
  - Response Limits | 47
  - Evaluate and Set Response Limits | 48
- Run Response Reports | 50
  - At-a-Glance Reports | 51
  - Trend Reports | 52
  - Service Level Reports | 52
  - Health Reports | 53
- Configure Live Health to Notify You of Problems | 55

**Appendix A: Configuring Application Response to Monitor Citrix Applications**

- Application Response in a Citrix Environment | 59
- Measure Response Time | 60
  - User Access to Your Citrix Applications | 61
  - AR Response Paths for Citrix Applications | 61
  - Client Names or User Names in Paths | 62
  - Trace Problems to Citrix Servers | 62
  - Organize Response Elements for Citrix Applications | 63
- Configure Application Response | 64
  - Step 1: Install AR Agents on Citrix Servers | 64
  - Step 2: Define Citrix-Specific Settings | 67
  - Step 3: Configure the Target Application | 70
  - Step 4: Organize Response Elements | 70
  - Step 5: Configure Live Health | 72
- Troubleshooting Tips | 72
- More Information | 75

**Appendix B: Troubleshooting Application Response**

- Guidelines | 77
- Error Messages and Agent Conditions | 78
- Common Symptoms | 84
- Information to Collect for CA Technical Support | 92

Index
Chapter 1: Overview

About This Guide

This guide describes how to do the following:

- Use eHealth Response to discover response elements, create response paths for those elements, and display response time data in eHealth reports.
- Get started with eHealth Application Response.
- Install, configure, and manage your eHealth Application Response (AR) agents.
- Configure response elements in eHealth and report on the data that eHealth Service Availability, Voice Quality Monitor (VQM), and Cisco® Service Assurance Agents (SAA) collect.

Audience

This guide is intended for eHealth administrators who are responsible for configuring eHealth to collect and report on response data. It is also intended for administrators who are installing AR agents and configuring and using Application Response.

Note: To configure response elements, you must have administrative permissions for the eHealth console. To configure and manage your AR agents, you must have administrative permissions for the eHealth Web user interface.

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.
Chapter 2: About eHealth Response

This chapter provides an overview of eHealth™ Response, and describes the components from which it collects data. It contains the following topics:

- What is eHealth Response
- How eHealth Monitors Response Time

What is eHealth Response

eHealth Response is an eHealth technology that 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® or Juniper® routers and other devices.

eHealth Response offers a comprehensive set of reports that help you manage your critical services and applications. You can also use Live Health™ to detect any performance problems in real time. These features enable you to detect degrading performance or declining availability of your critical services before those problems affect users, and maintain service levels by measuring the actual response times that end-users experience.

eHealth collects response data using one or more of the following products:

- eHealth Application Response (AR)
- eHealth Service Availability (SA)
- eHealth Voice Quality Monitor (VQM)
- Cisco IOS IP Service Level Agreements (SLAs)
- Juniper Real-Time Performance Monitoring (RPM)

Note: Cisco IOS IP SLAs were previously named the Cisco Service Assurance Agent (SAA)
Application Response

Application Response agents aggregate data and send it to eHealth. You do not discover AR agents and poll them for data. Response path elements appear in the database as after you initiate transactions. However, you must confirm that the AR agent data appears in the database to report on it with eHealth Response.

When you discover devices, eHealth adds elements for them to the poller configuration. This enables eHealth to poll the devices for performance data.

AR Agents

The AR agents that you install on Windows client systems monitor the applications running on those systems. You can configure and continually manage these agents and Web- or Windows-based applications from the Systems & Apps page of the eHealth Web user interface.

Note: eHealth r6.1 supports Application Response on Windows Vista platform.

You can specify the applications to monitor, define servers, discover connections, and perform many other agent management functions. You can also observe live transactions through the Agent Transaction Viewer (ATV) and run reports to show an application’s average response time.

For Application Response agent, application, and server management procedures see the Application Response eHealth Help.

For information about how to use Application Response to configure applications, see Configure Application Performance Using Application Response.

Monitoring Groups of Transactions

You can use Business Transaction (BT) Studio, an optional Application Response tool, to obtain more detailed information about your applications’ response times. While Application Response provides information about average response times for entire applications, use the eHealth BT Studio tool set to specify business-critical transactions or groups of transactions to monitor. You can then use Application Response to track performance data for those transactions, in addition to the performance of the application as a whole. This data appears in Application Response reports.

Transaction

A transaction is an application-specific task that may encompass several intermediary steps (windows or button clicks) or events.

Note: For information about BT Studio, see the eHealth Help, BT Studio.
Service Availability (SA) and Voice Quality Monitor (VQM)

Both Service Availability (SA) and Voice Quality Monitor (VQM) are plug-in modules for the eHealth SystemEDGE agent. After you discover the SystemEDGE agent systems you want to monitor, do the following:

- For SA, you use new Service Availability features to create tests that measure response time.
- For VQM, you use AdvantEDGE View to create response paths; then rediscover in response mode.

To access AdvantEDGE View and Service Availability

1. Log in to the eHealth Web user interface with administrative privileges.
2. Select the Systems & Apps tab.
3. Click AdvantEDGE View. The Service Availability options appear as links under the Service Availability heading.

Cisco IOS IP Service Level Agreements (SLAs)

Cisco IOS IP Service Level Agreements (SLAs) monitor network performance between a Cisco router and a remote device. IP SLAs provide performance information that you use for service level monitoring, troubleshooting, and resource planning. It measures response time for various network protocol devices, performance metrics, and statistics.

When you configure Cisco IP SLA with eHealth Response, the Cisco router generates traffic to specified network resources, and measures the availability of the resource and response time between the router and that resource. Cisco IP SLA can also measure important metrics such as latency, packet loss, and jitter, which are then stored in the eHealth database.

You can use this information to troubleshoot network problems, identify and analyze potential problems, and design future network topologies. Response data from Cisco IP SLA can appear in the eHealth reports described in Manage Response Using eHealth Reports, and can be used by Live Health to generate real-time alarms.

eHealth can also obtain data about HTTP or DNS transactions from routers that use Cisco IOS (Release 12.0T [5] or greater) to measure response time of these Internet applications. Response time of these applications includes the total elapsed time to perform a task at a connection level (such as downloading a web page), including network delay between the router and the HTTP or DNS server. You can display this data in eHealth reports. For more information about Cisco IOS IP SLAs, see your Cisco documentation.
Juniper Real-Time Performance Monitoring (RPM)

The Juniper real-time performance monitoring (RPM) feature monitors network performance between a Juniper router and a remote device. RPM generates probes between two network endpoints, and measures performance information, allowing you to perform service level monitoring, troubleshooting, and resource planning.

When you use eHealth Response to configure RPM, the Juniper router generates traffic between specified network resources, and measures performance information for those response paths. eHealth then polls the response paths, allowing you to monitor metrics including availability, packet response time, and jitter. If both the source and destination elements use the same Network Time Protocol (NTP) server, RPM records both one-way and round-trip data for the path. This information is then stored in the eHealth database.

You can use this information to track the quality of service a user experiences, troubleshoot network problems, and design future network topologies. Response data from Juniper RPM can appear in the eHealth reports described in Chapter 6, Using eHealth Reports to Manage Response, and can be used by Live Health to generate real-time alarms.

Juniper RPM defines jitter as the difference between the maximum response time and the minimum response time for a group of pings (Jitter = Maximum Response Time – Minimum Response Time). This jitter measurement may differ from that calculated by other devices.

For more information about Juniper routers and the RPM feature, see the documentation for your router.

How eHealth Monitors Response Time

To begin using eHealth Response, discover devices in your network on which Juniper RPM, Cisco IP SLA, and SystemEDGE agents reside. eHealth adds these devices to the poller configuration, which enables eHealth to poll them for performance data. The devices that you monitor for response time data are called response elements in eHealth.

You do not need to discover AR agents, but you must verify that the data associated with these elements appears in the database before you can report on it with eHealth Response.
Response Endpoints and Paths

A response destination is an element, such as a server, that processes transactions at the request of a response source, such as a client system. For example, you can obtain reports on the response time that a client application (response source) experiences from a web server (response destination). A response path measures responses between the source and destination, as illustrated in the following graphic:

![Response Path Diagram]

Response time is the time that it takes a response attempt to travel from the response source to the response destination and back. It represents the elapsed time between a user request and the server response. For VQM, the response source is called the *transmitter/receiver* and the destination is called the *reflector*.

Creating Response Paths

You may need to create response paths to test response time, depending on the product that you are using to collect data:

- With Cisco IP SLAs and Juniper RPM, you create response paths using the eHealth path manager.
- With Application Response, eHealth creates response paths automatically.
- With Service Availability (and the SystemEDGE agent), you create response tests using the Service Availability interface.
- With VQM, you use AdvantEDGE View to create the response paths; then rediscover in response mode.

When you discover devices that Cisco IP SLA, Juniper RPM, and SystemEDGE agents monitor, eHealth adds elements for these devices to the poller configuration. Then, you use these elements to create response paths. You can run various reports on your AR, Cisco IP SLA, Juniper RPM, and SystemEDGE paths to display application activity and response time.

Chapter 6 describes how to discover these response elements, and how to configure the elements for reporting.

**More information:**

Add Response Elements Using eHealth Response

Manage Response Elements Using eHealth Response
Chapter 3: Configure Application Performance Using Application Response

This chapter provides an overview of Application Response and explains how to install AR agents.

How Application Response Monitors Application Performance

Application Response uses AR agents to monitor application activity on remote client systems, collect and aggregate response data, and then send this data to eHealth through the AR Controller. To monitor and report on application performance, you need to specify an eHealth Response license for your eHealth system and install AR agents on Windows client systems in your infrastructure. The following graphic illustrates an Application Response configuration:
Understand the Role of the AR Controller

The AR Controller resides on the eHealth system. It sends configuration information to AR agents and also receives aggregated response time data from AR agents, which it saves in the eHealth database. eHealth automatically installs the AR Controller, but it does not have a user interface. It works as a background process.

Manage the Usage Queue Size

If you intend to use your eHealth system to support more than 500 active AR agents, you must set the AR Controller usage queue size to a value that is higher than the default value (500) by setting the MaxUsageQueueSize AR configuration variable (on the eHealth system) to the estimated total number of business transactions per minute multiplied by six. Set this value in the registry for eHealth Windows systems and in the ar.config file on eHealth Solaris and HP-UX systems. When eHealth receives the response data, it stores it in its database.

For example, if you have 5000 agents deployed, but only 2000 are licensed (meaning only 2000 agents can be active at one time), each agent records a business transaction at a rate of two transactions per minute. To calculate the value for MaxUsageQueueSize, multiply 2000 by 2; then multiply by 6. The result is 24000.

Monitor Applications with Application Response

Application Response provides a set of default applications and server definitions to allow you to begin monitoring application response time almost immediately:

- Mail
- Lotus Notes
- Oracle applications
- Microsoft Outlook
- PeopleSoft
- SAP R/3
- Telnet
- Web (including Web transactions performed using Microsoft Internet Explorer and Netscape Navigator)

When you use Application Response out-of-the-box, you can monitor an application’s response time by selecting and enabling one of these default applications with or without specifying a server. If you do not specify a server, Application Response uses a default server definition to measure network and server time for application activity. Out-of-the-box indicates that you are running eHealth Response and you have installed AR agents, and little or no other configuration is required.
Application Response measures the response time of activity between the application and server. Default rules specify the connections and transactions that it monitors.

You can also define other applications that you want Application Response to monitor, such as DNS and custom applications, using the Systems & Apps page of the eHealth Web user interface.

**Viewing Application Information**

You can view information for applications in several ways:
- eHealth Web user interface
- Agent Transaction Viewer (ATV)
- Response reports
- eHealth BT Studio

**Use Default Applications and Servers**

When you enable a default application, Application Response monitors the application executable using a default server to collect response time data. Response reports display a pathname that contains the names for the client, application, module, and server. A module is a group of related transactions. In reports, Application Response aggregates performance data for all transactions that belong to a module.

If you are using default servers, the default server name appears near the end of the pathname. If you want specific server name to appear in the path of reports or if an application uses multiple servers and you want to track response time for each server individually, then you must create new servers or attach other servers to your application. For information about how to create new servers and attaching different servers for your applications, see the Application Response Web Help.

**More information:**

Verify That Your Application Response Paths Appear in eHealth

**Default Servers for Terminal Services**

Application Response provides a default server for terminal server applications (also known as thin-client applications). In a terminal services environment, a client system communicates with a terminal server, which, in turn, communicates with an application server. AR agents can monitor application activity and response time for these types of configurations.

If you want to monitor terminal server applications, you must obtain an Application Response for Thin-Clients and Terminal Servers (TS) agent license that supports the number of AR agents that you want to install.
How Application Response Monitors Application Performance

The AR agent measures application performance by monitoring the actual activity of an application. By default, it provides overall response information. When you write rules with BT Studio, you define specific business transactions to measure.

When AR agents aggregate the data that they collect and send it to eHealth, you can do the following:

- **Monitor application performance.** AR agents collect actual response data for individual user transactions and aggregate them into an average response time per application for each user. Sort data by user or group, by application, or by time of day.

- **Identify the source of performance problems.** While monitoring end-user activity with AR agents, you can observe the three following parts of total response time:
  - Client time - Processing time for the application client.
  - Server time - Processing time for the application server, which includes processing time for any back-end servers.
  - Network time - The time required to transmit information between the application client and server.

This information helps identify which part of the infrastructure is contributing the most to slow performance. When the agents detect a performance problem, use eHealth reports to identify the source of the problem and drill down to additional reports for more detailed information.

- **Correlate response performance to system and network performance.** If you are already monitoring system and network performance through other eHealth components, you obtain a more comprehensive view of this performance by monitoring application response time with AR agents.

AR agents monitor terminal server applications and applications running in standard client/server configurations. They can monitor the performance of most Windows-based or Web-based applications whose clients use Microsoft TCP/IP connections. For each application, the AR agent observes transactions that users perform and tracks the amount of time required to complete each one. The agent then calculates an average application response time for use in eHealth reports.
Prepare for AR Agent Configuration

Before you install AR agents, do the following:

- Verify that you have installed an eHealth Response license and that you have met the system and Web browser requirements outlined the AR.README file in your eHealth installation directory.
- Obtain and install AR or TS licenses for your AR agents. For information about these license types, see the next section, License Application Response and AR Agents. For information about installing licenses, see the eHealth Help, Administration.
- Verify that the systems on which you plan to install AR agents meet the agent system requirements outlined in the AR.README file located in your eHealth installation directory.

License Application Response and AR Agents

When you add an eHealth Response license to your eHealth system, Application Response is automatically enabled. With this license, you can access the Application Response agent management tool on the Administration page of the eHealth Web user interface. You must obtain a license that supports the number of AR agents that you want to install on Windows client systems or terminal servers in your infrastructure so that the AR Controller can accept data from them. The following sections describe the types of agent licenses, how agents obtain licenses, and how you can view the license status of your agents.

AR and TS Licenses

To be able to monitor application response time in different environments, you must obtain a License Request form to obtain the necessary licenses.

- To monitor application response time within a standard client/server environment, you must obtain an Application Response agent license.
- To monitor application response time within a terminal services environment, you must obtain an Application Response for Thin-Clients and Terminal Servers agent license. You add these licenses to your eHealth system.
- To monitor applications in a standard client/server environment, you install one agent on each remote client system that is running applications that you want to monitor. Determine the number of AR agents from which you plan to actively collect data at one time and submit a License Request form that specifies this number.
- To monitor terminal server applications, you install one AR agent on each terminal server in your infrastructure. You do not install AR agents on the individual thin-client systems. Determine the number of AR agents that you want to install and submit a License Request form that specifies this number.
Performance Considerations

Application Response performance varies depending upon the operating system on which you run eHealth. For example, when eHealth resides on a Solaris or HP-UX system, the AR Controller on that system may be able to process information from a greater number of AR agents than an AR Controller that resides on a Windows system. Before you determine the number of AR agents that you plan to license, consider the operating system on which you are running eHealth.

**Note:** For information about viewing license information and reallocating licences, see the eHealth Help, Application Response.

Install, Configure, and Deploy AR Agents

To install new AR agents, you use the AR Agent Publisher to create agent installation programs. You run these programs on target Windows client systems to install the agents. The following section provides information about agent installation programs and how to generate them.

**More information:**

Upgrade AR Agents and Modify Advanced Settings

Uninstall AR Agents

Get Started

If you have not already done so, you must install eHealth on a Windows or UNIX system, as described in the eHealth Installation Guide. Application Response supports Internet Explorer 5.0-6.0SP2. You must have an eHealth Response license and an AR agent license that supports the number of agents that you plan to run at a given time. If you plan to use Live Health, you must also install a Live Health license. For complete instructions on entering licenses, see the eHealth Help, Administration.

Plan Your Time

If you have already installed eHealth and obtained the necessary licenses, plan to spend a few hours configuring your new application, creating the agent installation program, deploying a test agent, and running a report to ensure that your agent is working. After you complete these steps, you will need to spend another few hours deploying your agents widely, grouping your agents, and optionally configuring Live Health.
The Configuration Process

The process of configuring Application Response to monitor your applications can involve the following steps:

**Note:** some of the procedures and steps in this section depend on the type of application you are configuring.

- Use the default installation program.
- Create the agent installation program.
- Install Agents on Terminal Server Systems.
- Deploy a AR agents client systems across your infrastructure using email.
- Uninstall AR agents.

For procedures to add an application, upgrade an AR agent, import a rule set, add a server, and other agent and application management tasks, see the eHealth Help, Application Response.

**Note:** After you complete the procedures in this chapter, you can run response reports on your elements. For procedures and information, see Prepare to Run Response Reports.

Use the Default Agent Installation Program

If you are running the AR Agent Publisher on the eHealth system or on a system in which an AR agent already exists, you can select Generate a default AR Agent Installation program. The Agent Publisher targets the known AR Controller or uses the current agent settings to create a default agent installation program. When you select this option and click Next, the Start Generating Program dialog appears, bypassing the dialogs in which you would otherwise specify settings.

**Note:** If you want to install an agent on the system on which you are currently running the Agent Publisher, but an AR agent does not currently exist and it is not the eHealth system, you must generate a new agent installation program and then run it on this system.

Create the Agent Installation Program

To install new AR agents, you use the AR Agent Publisher to create an agent installation program. You run the AR Agent installation program on target Windows client systems to install the agents. You can also use the AR Agent Publisher to create new agent installation programs with new rules. You can generate a single installation program and send it to one or more target systems.

The AR Agent Publisher runs on Windows systems only. Download it from the Download page on the Web user interface as follows.
To use the AR Agent Publisher to create the agent installation program

2. Click Run. The Welcome dialog appears.
3. Select Generate an AR Agent Installation Program; then click Next.
4. Read the Software License Agreement, if it appears. If you accept the terms, click Yes to continue.
5. In the Edit Controller Information dialog, enter the name of the eHealth system in the Hostname field (that is, the host name of the system on which eHealth resides) and accept the default values in the Port and Agent Port fields; then click Next.

    **Note:** For the initial deployment, leave the Name field under Agent Set blank. When you install additional agents and set up grouping, use this field to associate agents with groups.

6. In the Options for Agent Install dialog, deselect Silent Agent Install, and then do one of the following:
   - (Microsoft Outlook): Select Netscape Navigator.
   - (Custom Applications): Accept the defaults.
   Click Next.
7. In the Agent Extensions dialog, click Next. After you deploy your test agent, you can return to the Agent Publisher and create a version of the agent that monitors Java applications and applets.
8. In the Enter Target Directory for Agent Install dialog, leave the field blank and click Next. By default, the program installs the agent for the client machine on the boot drive and creates an ehealth/agent/response directory.
9. In the Choose Destination Location and Program name dialog, accept the default name and location, or specify new values; then click Next.
10. In the Edit Agent Host Names dialog, click Next.
11. In the Start Generating Program dialog, review the information. If you want to change your settings, use the Back button.
12. When you are satisfied with your settings, click Finish. The AR Agent Publisher creates a file called ARInstl.exe. This is the file that you will deploy to your client system to install the AR agent.
13. Before you distribute the file, enable eHealth to monitor the application by doing the following:
   b. Scroll to the application and select the checkbox; then click the Enable Selected Application button above the list.
   c. Click OK. The screen refreshes and re-displays the Application list. An icon should no longer appear in the Disabled column for the application.
Install Agents on Terminal Server Systems

When terminal server administrators receive the agent installation program executable file, they must do the following:

1. Save the file to a directory on the terminal server system.
2. Use the Add/Remove Programs dialog to open the executable file and install the agent on the server.

To help ensure that the agent is properly installed on the terminal server, use the following procedure.

**To install an AR agent on a terminal server system**

1. On the desktop, go to Start, Settings, Control Panel.
2. Double-click Add/Remove Programs. The Add/Remove Programs Properties dialog appears.
3. Select the Install/Uninstall tab; then click Install. The Install Program From Floppy Disk or CD-ROM dialog appears.
   - **Note:** The agent executable file is too large to distribute on a floppy disk. However, you use this program to navigate to a dialog in which you can browse to access the directory in which you saved the file.
4. Click Next. The Run Installation Program dialog appears.
5. Click Browse. The Browse dialog appears. Navigate to the directory in which you saved the executable file.
6. Select the file and click Open. The Browse dialog closes and the Run Installation Program dialog displays the agent executable path.
7. Click Finish to run and complete the agent installation.
8. If necessary, reboot your system:
   - After you run the installation program executable on the target system, the system may require a reboot.
   - If you did not select Silent Agent Install, the installation program informs you if the reboot is required, and allows you to reboot immediately or at a later time.

If you encounter installation errors, check the ARAgentInstall.log file in your temp directory. This file stores system information, installation information, and installation errors.

When you install AR agents, they register automatically with the AR Controller. The agent information appears on the Agent List page under AR Agent Management on the eHealth Web user interface.
Deploy AR Agents to a Limited Number of Client Systems

When you install an agent on a system, it becomes an AR client. To deploy agents to a limited number of client systems, you can use email.

**To distribute the AR agent to a Windows client system**

1. Create an email message and attach the AR agent installation program (ARInstl.exe). In the email, instruct the user of the client system to do the following:
   a. Save work and close open programs. (Explain that if a reboot is necessary, the installation program will prompt the user.)
   b. Double-click the executable to install the agent. This process may take up to 15 minutes. When the agent is installed, the client system becomes an AR agent client system.

2. After you send the email, confirm that the user has installed the agent on the client system; then do the following:
   a. If you are not already logged into the eHealth Web user interface, open a Web browser, log in, and access Application Response on the Systems & Apps page.
   b. Ensure that your Web browser is set to update with every visit to a page. Select Tools, Internet Options. In the Internet Options dialog, select the General tab; then click Settings under Temporary Internet Files. In the Settings dialog, select Every visit to the page; then click OK. Click OK to close the Internet Options dialog.
   c. Select Agents and make sure that the test system name appears in the list. If it does not appear, click the Refresh button.
   d. If ON does not appear in the State column for an agent, select the check box next to the name in the list; then click the Start Selected Agents button above the list. After the screen refreshes, the Status column should display a green icon.

3. Verify that the agent is working by enabling it to perform transaction logging. Select the check box to the left of the agent name; then click the Start Transaction Logging for Selected Agents button above the list. The screen refreshes and displays a checkmark in the Transaction Logging column.
   **Note:** An agent cannot log transactions if it is not licensed. Verify that a checkmark appears in the Licensed column. If one does not, refer to the Web Help for information about how to make a license available for the agent.

4. Contact the user of the AR agent client system and instruct the user to open a new Web browser and access the Web site for which you created the application. This enables the agent to capture the data specific to the new application and send it to eHealth. This is necessary to ensure that transaction data appears when you perform the next step.
   **Note:** If the client system is running Terminal Services, see Uninstall AR Agents.
5. To confirm that the eHealth system is receiving transaction data, view the agent transaction log:
   a. On the Agent List page, select the check box to the left of the agent name; then click the View Transaction Logs of Selected Agents button above the list.
   b. Click OK to launch the ATV. The Agent Transaction Viewer window appears.
   c. Click the Get Transaction Data from Agent button at the top of the screen. The screen refreshes and displays the list of Web transactions (for the new application) that have been performed on the client system.

Upgrade AR Agents and Modify Advanced Settings

The Advanced Settings page enables you to specify upgrade information for agents and modify global Application Response settings. To access this page, on the Systems & Apps page under Application Response, click Advanced Settings.

Advanced Settings Page

There are three sections on the Advanced Settings page.

General

The fields in this section display the default settings for the eHealth system (where the AR Controller resides). You can modify these settings if you do not want to use the default ports for the following fields:

Controller Port
  10182

Agent Port
  10165

Proxy Port
  10166

Console Port
  10183

In a terminal services setting, if you want to monitor application activity by user, select the Use Client User Names in Terminal Server Mode check box. Application Response identifies the application transactions by client user name. When this check box is not selected, Application Response uses client system hostnames to identify the transactions to monitor. In other words, it tracks the transactions by each client system, not by the users of those systems.
Controller

When you select Enable Transaction Logging, this global setting enables all AR agents to log transactions. The setting takes effect when the agents heartbeat in to the Controller.

If you upgrade your agents and you had enabled global transaction logging, you can disable global logging by editing the Windows registry setting for the FirstSense, TransactionLogging key. Set the key to zero (0) to disable global logging; then, you can specify transaction logging on a per-agent basis.

Agent Upgrade

This section replaces the standalone Agent Configuration Manager for Windows and UNIX. You now use this portion of the Advanced Settings page to specify your agent upgrade settings, regardless of whether eHealth resides on a Windows or UNIX system.

To upgrade agents on your remote client systems

2. Click Run. The Welcome dialog appears.
3. Select Generate an AR Agent Installation Program; then click Next.
4. Read the Software License Agreement, if it appears. If you accept the terms, click Yes to continue.
5. In the Edit Controller Information dialog, enter the name of the eHealth system in the Hostname field. (You do not have to modify the values in the Port and Agent Port fields unless you are using values other than the default values.) Click Next.
6. In the Options for Agent Install dialog, accept the defaults and click Next.
7. In the Agent Extensions dialog, click Next.
8. In the Enter Target Directory for Agent Install dialog, you do not have to specify a value. The program will upgrade the agent in the directory in which it was originally installed.
9. In the Choose Destination Location and Program Name dialog, accept the default value for the installation program name and destination.
10. In the Edit Agent Host Names dialog, to upgrade specific agents, select Affect only specific hosts and list the hostnames of the target systems on which the agent is to be upgraded. If you do not list specific systems, the agent installation program executes on all AR agent systems.
11. In the Start Generating Program dialog, review the settings and click Finish. The AR Agent Publisher creates a file called ARInstl.exe. This is the file that you will deploy to your client system to install the AR agent.
12. Provide access to the agent installation program executable. The target Windows systems (on which the agents must be upgraded) must have access to the directory in which the new agent installation program executable will reside. Verify that this directory is shared. For specific instructions, refer to the Application Response Readme file (Readme.AR).

13. Enable the agent upgrade by specifying settings on the Advanced Settings page, as the following table describes. When you save your changes, the AR Controller is updated. When users of the remote client systems run the new agent installation program, the agents are upgraded when they heartbeat into the Controller.

**Note:** The agents will not upgrade until the time you specify on the Advanced Settings page.

The following table describes the settings required for each field in the Agent Upgrade section of the Advanced Settings page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version</td>
<td>The agent version is identified by the eHealth version (or eHealth Release number). Specify the eHealth version that you are upgrading to, including the build number.</td>
</tr>
<tr>
<td><strong>To view the agent version number</strong></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>On the Download page (Application Response &gt;Download), right-click the Agent Publisher download link and select Save Target As and save it to your desktop. (This step ensures that you are viewing the latest version in the event you have an old version on your desktop.)</td>
</tr>
<tr>
<td>2.</td>
<td>On the desktop, right-click the Agent Publisher shortcut and select Properties.</td>
</tr>
<tr>
<td>3.</td>
<td>On the Version tab, under Item name, select Product Version. The version number appears in the Value field.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter this value in the Agent Version field on the Advanced Settings page.</td>
</tr>
<tr>
<td>Script</td>
<td>Specify the location of the AR Agent Publisher executable file using a Universal Naming Convention path such as \servername\sharename\path\filename.</td>
</tr>
<tr>
<td>Script Arguments</td>
<td>This field is not used at this time.</td>
</tr>
<tr>
<td>Time</td>
<td>Specify the time for the agent upgrade to take place. If the client systems are in a time zone that is different from that of the eHealth system, specify the client system time.</td>
</tr>
</tbody>
</table>
Uninstall AR Agents

To remove agents from target systems, select Generate an Uninstall program for existing AR Agents on the Welcome dialog of the AR Agent Publisher. The AR Agent Publisher places a generated uninstall executable file in the path that you specify. You can then specify the hostnames of the systems on which you want to run the uninstall program. For more information, refer to the AR Agent Publisher web Help.

**Note:** When you run the uninstall executable on a client system, the system is restarted automatically without warning.
Chapter 4: Add Response Elements Using eHealth Response

This chapter explains how to use eHealth to discover SA, VQM, Cisco IOS IP SLA, and Juniper RPM devices. It also explains how to create response destination elements and paths that enable eHealth to display response time data in eHealth reports. It includes the following sections:

- Overview of the Discover Process
- Create Response Destination Elements
- Create Response Paths
- Verify That Your Application Response Paths Appear in eHealth

Overview of the Discover Process

To discover response sources, you discover SNMP agents (Cisco IP SLA, Juniper RPM, and SystemEDGE agents) using response discover mode. Response sources and destinations are used as endpoints when you create response paths. When you save the results of this discover process, eHealth creates an entry in the database for each response element.

**Note:** In addition to the SNMP agents it discovers as response elements, eHealth also discovers any pre-existing RFC2925 (Disman) response paths on Cisco or Juniper routers. These response paths are polled as plain data elements by eHealth. They are not managed the same way as the response paths you create using eHealth Response. If you do not want to discover these pre-existing response paths, edit the poller configuration before saving the results of the discover process.

When you run the discover process, eHealth looks for SNMP agents at ports 161 and 1691 by default. You can configure eHealth to search for SNMP agents on other agent ports using Discover Policy parameters.
Schedule a Discover Job

To verify that the response element information is current, you can schedule the discover process to run on a regular basis. When you schedule a discover job, eHealth automatically discovers any new SNMP agents installed on devices within the IP address range you are monitoring.

Create Response Destination Elements

After you discover Cisco IP SLA or Juniper RPM response elements and save them to the eHealth database, you must create response destination elements using the eHealth path manager. You use these destination elements to define response paths.

Note: You do not perform this procedure for eHealth SA and VQM. For SA and VQM, you create response paths using Service Availability and AdvantEDGE View.

Destination elements indicate one endpoint of a response path that eHealth monitors. The other endpoint is an existing response source. eHealth monitors activity between the endpoints you specify, and displays this information in reports.

You can create response destination elements from routers and servers you have previously discovered, or you can specify the IP address of a new element that does not yet exist in the poller configuration.

To create response destination elements

2. Click Path/PVC Manager. The Path/PVC Manager dialog appears.
3. Select Response Path under List Elements by Type.
5. Click Add Destination. The Add Destination Element dialog appears.
6. Do one of the following:

- Create response destination elements from existing elements as follows:
  a. Select Create Response Destinations from existing elements.
  b. Select one or more elements from the Select Elements list. To search for a known element, specify the initial characters of the element name in the Search for Name field, then press Enter.
  c. Click Apply. The selected elements appear in the list of path destinations in the Add Paths dialog. This dialog appears in the background on your screen.
  d. Click OK to save these elements as destination elements and to close the Add Destination Element dialog.
  e. Go to Create Response Paths.

- If you want to add information for a new response element that does not currently reside in the poller configuration, and that you want to designate as a response destination, create a new response destination element as follows:
  a. In the Add Destination Element dialog, select Add a new Response Destination. The Add Destination Element dialog displays new fields.
  b. Specify a name in the Endpoint Name field for the element. 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, dashes (-), periods (.), underscores (_), colons (:), and slashes (/).
    **Note:** eHealth reports often truncate the element names, therefore, 30 characters is recommended. If you use a combination of single-byte and double-byte characters, the total length cannot exceed 64 bytes.
  c. (Optional) Specify an alias name in the Endpoint Alias field for the element. The alias name has the same length and character restrictions as the element name.
  d. Specify the IP address of the response destination in the IP Address field.
  e. (Optional) Specify the unique network name of the destination in the Host Name field. To add the destination element, DNS must be able to resolve this hostname.
  f. Click Apply. eHealth adds the new element to the list of path destinations in the Add Paths dialog.
  g. Click OK. The new element is saved as a destination element.
Create Response Paths

Once you have discovered source endpoints and created response destinations, you must create response paths for your Cisco IP SLA and Juniper RPM elements. eHealth adds these paths to the poller configuration, and uses them for active response testing and for reporting on the response data collected.

Application Response paths appear in eHealth automatically when you configure your AR agent information through the eHealth Web user interface. You should verify that these paths appear.

More information:

Verify That Your Application Response Paths Appear in eHealth

Note: You use AdvantEDGE View to create VQM paths. For instructions, see the Create Voice Quality Paths eHealth Help topic. For SA elements, you use Service Availability to create tests. For instructions, see the eHealth Help.

When you create response paths with the path manager, you select a protocol, one or more sources, and one or more destinations. The following table shows the protocols that eHealth Response supports and the types of agents that monitor these protocols.

Note: When creating response paths for Juniper RPM, confirm that both the source and destination elements use the same Network Time Protocol (NTP) server.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Service Availability</td>
</tr>
<tr>
<td>(Windows only)</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td>Service Availability</td>
</tr>
<tr>
<td>DHCP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>DNS</td>
<td>Cisco RTTMON and Service Availability</td>
</tr>
<tr>
<td>FILE I/O</td>
<td>Service Availability</td>
</tr>
<tr>
<td>FTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>HTTP</td>
<td>Cisco RTTMON GET, Cisco RTTMON Advanced,</td>
</tr>
<tr>
<td></td>
<td>and Service Availability</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Service Availability</td>
</tr>
<tr>
<td>IMAP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>jitter</td>
<td>Cisco RTTMON and Juniper ICMP Echo</td>
</tr>
<tr>
<td>LDAP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>MAPI (Windows only)</td>
<td>Service Availability</td>
</tr>
</tbody>
</table>
Create Response Paths

Add Response Elements Using eHealth Response

Note:
The protocols listed in the Agent column for Service Availability and eHealth VQM are not selections in the path manager.

To create response path elements

1. From the Add Paths dialog, select a protocol from the Create Paths That Support Data Collection Using This Protocol list. When you select a protocol, it populates the Select One Or More Path Sources list. This list shows only those sources that support the protocol that you select.
2. Select one or more sources from the Select One Or More Path Sources list.
3. (Optional) Modify the values for the path properties by doing the following:
   a. Select the property under Attribute. eHealth displays a brief description of the selected property in the Description field.
   b. Specify a new value in the Value field. The number, type, and default values of the properties differ for each.
4. Select one or more path destinations from the Select One Or More Path Destinations list by using one of the selection methods described in Step 2. If response destinations are not listed, or if the list does not contain the element that you want to use, click Add Destination.
5. At the bottom of the Add Paths dialog, refer to the note that shows the number of paths that eHealth will build with your choices. This number includes any paths that already exist.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS</td>
<td>Service Availability</td>
</tr>
<tr>
<td>NNTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>Ping</td>
<td>Cisco Ping, Cisco RTTMON, Disman ICMP Echo, Service Availability, and Juniper ICMP Echo</td>
</tr>
<tr>
<td>POP3</td>
<td>Service Availability</td>
</tr>
<tr>
<td>Round-Trip Email</td>
<td>Service Availability</td>
</tr>
<tr>
<td>SMTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>SNMP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>SQL Query</td>
<td>Service Availability</td>
</tr>
<tr>
<td>TCP Connect</td>
<td>Cisco RTTMON and Service Availability</td>
</tr>
<tr>
<td>TFTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>UDP</td>
<td>Cisco RTTMON</td>
</tr>
<tr>
<td>Virtual User (Windows only)</td>
<td>Service Availability</td>
</tr>
<tr>
<td>VoIP</td>
<td>eHealth VQM</td>
</tr>
</tbody>
</table>
eHealth creates path elements between each source and destination that you select. For example, if you select three sources and five destinations, eHealth creates 15 path elements, unless a path already exists. Confirm that this is what you want to do.

6. Do one of the following:
   – Click Apply to save the response path elements and refresh the window so you can create other response path elements.
   – Click OK to save the response path elements and close the Add Paths dialog. The Path Builder Results dialog appears.

   **Note:** If the path needs a hostname for one or more destinations, the Path Builder Results dialog indicates that eHealth detected invalid destinations and lists the destinations for which you must specify a hostname.

7. Review the following:
   – Number of paths that eHealth created
   – Names of the duplicate paths that it did not create
   – Names of paths that it did not create because they exceed the maximum number of paths for a response source

8. Click OK to close the Path Builder Results dialog; then click Close to close the Path/PVC Manager dialog.

9. You must click OK or Apply in the Poller Configuration dialog to save the path sources and destinations that you selected. When you click OK or Apply, eHealth creates the response paths.

   **Important!** If you click Cancel in the Poller Configuration dialog, you lose all of the work that you have performed since you opened this dialog.

### Response Element Naming Conventions

When you discover response source endpoints, create response destinations from existing elements, or create response path elements, eHealth names the response elements according to the format defined in the following table:

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Source</td>
<td>systemName-RS</td>
</tr>
<tr>
<td>Response</td>
<td>elementName-RD</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td>Path</td>
<td>sourceElementName-DestinationElementName-protocol-AP</td>
</tr>
</tbody>
</table>

eHealth creates a unique element name for each element. If you create response path elements that are identical except for the value that you assign to a polling variable, eHealth appends a letter to create a unique element name. For example, if you have a path element named router21-webserver1-ciscoPing, you can create an identical element that uses a different packet size. eHealth names the new element router21-webserver1-ciscoPing-A.
Verify That Your Application Response Paths Appear in eHealth

To verify that your Application Response paths appear in eHealth, you can view them through the Poller Configuration dialog. Application Response paths consist of a client, application, module, and server name, as shown in the following graphic. eHealth appends an AP to the end of these paths to indicate that they are Application Paths.

When you configure Application Response paths, the path name cannot exceed 64 characters. If a path name does exceed this limit, eHealth generates an error and does not include response time data for this path in reports. When you create names for applications, modules, and servers using AR Agent Management, each name should not exceed 15 characters.

Interpret Polling Errors on Response Path Elements

Often, after you create a response path, you must perform other steps to properly configure the response source to collect data or validate the information specified for the path such as the IP address. If a path is polled successfully, but it returns all zero data or is unavailable, the path is probably not configured correctly. eHealth can report these conditions to help you troubleshoot improperly configured paths.

For response paths configured on Cisco routers, eHealth displays an error message in the console window when the number of consecutive successful polls that return all zero data exceeds the value of the NH_RTR_ZERO_DATA_POLLS. The default value of this variable is 6. After six such polls, eHealth displays the message and resets the counter. You can decrease the value to obtain the error message after fewer polls that meet this criteria, or increase it to obtain the message after more consecutive polls that meet this criteria.

For response paths configured on Juniper routers, eHealth may display one of two error messages:
Interpret Polling Errors on Response Path Elements

- **Ping Response Probe juniper-ICMP-AP did not run on remote machine** – Indicates that the test did not run. If this error occurs on every poll cycle, the destination element is not reachable from the router. You should verify the IP address of the destination. If the error occurs only occasionally, it generally indicates the router did not have the resources to run the test (it was too busy routing traffic).

- **Ping Response Probe juniper-ICMP-AP ran on remote machine, but did not receive any responses** – Indicates that the test ran but did not receive a response. If this error occurs consistently, the destination element probably does not exist on the network. You should verify that the destination exists and the path is configured correctly. If the error occurs sporadically, the destination is occasionally not responding to the ping. It may be offline for certain time periods.
Chapter 5: Manage Response Elements Using eHealth Response

This chapter describes how to use the Poller Configuration dialog to manage the response path elements in your configuration. It includes the following sections:

- Manage Response Path Elements
- Modify Response Path Elements
- Modify Source and Destination Elements
- Delete Response Elements

Manage Response Path Elements

Use the Path/PVC Manager dialog to manage the response path elements in your configuration.

To display the Path/PVC Manager dialog

2. Click Path/PVC Manager. The Path/PVC Manager dialog appears.
   
   **Note:** The title of the Path/PVC Manager dialog indicates the Set Element Filter setting in the Options dialog. If you have not set a filter, the dialog lists all paths.
3. Under List Elements of Type, select Response Path.
4. (Optional) Manage your view of the elements in the list by sorting the list of elements. Specify a sorting method under Sort List by:
   - Select Alias to display the elements in alphanumeric order according to their aliases. This option only appears if you selected Show Alias Names in the Options dialog.
   - Select Name to display the elements in alphanumeric order according to their element names.
   - Select Source to list the paths by their response source. The paths appear in alphanumeric order according to their element or alias names.
– Select Destination to list the paths by their response destination. The paths appear in alphanumeric order according to their element or alias names.
– Select Protocol to list the paths by the protocol setting.
– Select Poll Rate to display the elements according to their poll rate.
– Select Agent Type to display the elements in alphanumeric order according to their agent type.

5. By default, eHealth displays all response path elements that exist in your poller configuration. Optionally, customize the list by selecting one of the following under Show:
– Select All to display all path elements.
– If you are building new paths, select Newly Added to display only the newly created paths that have not yet been saved in the Poller Configuration dialog.
– If you want to display only the response path elements that Live Exceptions is not monitoring, select LE Unmonitored.

When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list. However, you can disable monitoring for one or more specific elements.

6. Do one of the following:
– To save the elements that are currently displayed in the dialog and to save their information in the paths.cfg.log file in the log directory of your eHealth installation, click Save List To File.

The paths.cfg.log file is an ASCII file with tab-separated fields, as described in the following table. If a field does not apply to the element, that field remains empty.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Specifies the order of this element in the file.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the element name; or, if you selected Show Alias Names, when you save this file, this field specifies the alias that you assigned to this element.</td>
</tr>
<tr>
<td>Response Source</td>
<td>Specifies the response source element for the path element.</td>
</tr>
<tr>
<td>Response Destination</td>
<td>Specifies the response destination element for the path element.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol used to test the response of the path.</td>
</tr>
<tr>
<td>Poll</td>
<td>Specifies the polling rate that eHealth uses to poll the element.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>Specifies the type of data collected by the path element.</td>
</tr>
<tr>
<td>Element</td>
<td>Specifies the element name of the path.</td>
</tr>
</tbody>
</table>
To save newly added paths, click Close on the Path/PVC Manager dialog and then click Apply or OK in the Poller Configuration dialog to save your changes.

**Modify Response Path Elements**

You can use the Path/PVC Manager dialog to modify Cisco IP SLA and Juniper RPM response path elements in the following ways:

- Change its alias name, source, or destination.
- Specify a new protocol (agent type).
- Specify new settings and limits for the protocol.
- Change its response polling variables.

**Note:** You can also use the path manager to modify Service Availability elements, but CA recommends that you use the Service Availability interface.

**To modify a single response path element**

2. Click Path/PVC Manager in the Poller Configuration dialog. The Path/PVC Manager dialog appears. The title of the dialog indicates the Set Element Filter setting in the Options dialog.
   
   **Note:** To access the Options dialog, select Setup, Options on the console.

   - If you have not set a filter, the title indicates that the Path Manager dialog lists all paths.
   - If you have set a filter, the title indicates the group name.
3. Select an element and click Modify. The Modify Path Element dialog appears.
4. (Optional) Do any of the following:
   - Change the name by replacing the text in the Name field.
   - Specify an alias name by specifying text in the Alias field.
   - Select a protocol from the Agent Type list.
   **Important!** Confirm that the Agent Type you specify is appropriate for the selected response element. Changing the Agent Type to an unsupported protocol can result in polling errors.
   - Specify another source or destination by replacing the text in the Source or Destination fields, respectively. To select an element from a list, click Browse next to either field.
   - When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list. Disable Live Exceptions monitoring for this element by deselecting Monitor under Live Exceptions.
By default, Live Exceptions monitors elements using the time zone of the eHealth server. Specify a different time zone for the element by selecting a time zone from the Time Zone list.

**Note:** The Live Exceptions fields only appear if you have a Live Health license. For more information, refer to the eHealth Help, Live Health.

- Under Response Polling Variables, turn polling off, or select Normal, Slow, or Fast polling for the element.
- Specify different settings for attributes. Select the attribute in the Attribute list and specify another value in the Value field.

5. Do one of the following:
   - Click Apply/Next to change the path element and display the next element in the list.
   - Click OK to change the path element and close the Modify Element Path dialog.

6. Click Close to close the Path/PVC Manager dialog.

7. Click OK or Apply in the Poller Configuration dialog to save the changes.

**To modify multiple response path elements**

1. In the Poller Configuration dialog, click Path/PVC Manager. The Path/PVC Manager dialog appears. The title of the dialog indicates the Set Element Filter setting in the Options dialog.
   - If you did not set a filter, the title indicates that this dialog lists all paths.
   - If you have set a filter, the title indicates the group name.

2. Select multiple elements and click Modify. The Modify Path Elements dialog appears.

3. (Optional) Change the polling rate for the elements by selecting Change Poll To, then:
   - Select Off to turn off polling for the elements.
   - Select Normal to poll elements at the Normal rate.
   - For statistics elements, select Slow to poll elements at the Slow rate.
   - For statistics elements, select Fast to poll elements at the Fast rate.
   If a path element does not support a polling interval setting, eHealth does not make that setting selectable. For more information about polling rates, refer to the section on changing polling rates in the *eHealth Administration Guide*.

4. Specify in the Retries field the number of times you eHealth to send requests to an element before giving up on a poll.

5. Specify in the Timeout field the amount of time (in microseconds) that you want to wait before timing out a poll for an element. (Specify an integer value.)

6. (Optional) Change the names of the selected elements by selecting Change Element Name. Specify the part of the name that you want to replace in the Replace sub-string field. Specify the new part of the name in the with field. The name strings are case sensitive.
7. (Optional) Change the alias names of the selected elements by selecting Change Alias Name and following the instructions in Step 8.

8. (Optional) Change the community string for the elements that you selected by selecting Change Community. Specify the old community string in the from field; then specify a new community string for which you have write permission in the to field. Specify the entire community string. The community strings are case-sensitive.

9. (Optional) Specify a shared response time target by selecting Set Limit To and specifying a number in the adjacent field.

10. (Optional) Specify another response source by selecting Change Source. Specify the element name of the current source element in the from field and the element name of another source element in the to field. To find source element names, switch to the Poller Configuration dialog; then copy and paste between the dialogs.

11. (Optional) Specify another response destination by selecting Change Destination. Specify the element name of the current destination element in the from field and the element name of another destination element in the to field. You can copy element names from the Poller Configuration dialog.

12. (Optional) Specify another IP address to use for the source element by selecting Change Source IP. Specify the current source element’s IP address in the from field and the IP address of another source element in the to field.

13. (Optional) Specify another IP address to use for the destination element by selecting Change Destination IP. Specify the IP address of the current destination element in the from field and the IP address of another in the to field.

14. (Optional) Change the Live Exceptions monitoring status by doing one or both of the following:
   - When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list. Disable Live Exceptions monitoring for this element by selecting Monitor and No under Live Exceptions.
   - By default, Live Exceptions monitors elements using the time zone of the eHealth server. Select a different time zone for the elements by selecting Modify Time Zone and selecting a time zone from the Time Zone list.

   **Note:** The Live Exceptions fields appear only if you have a Live Health license. For more information, refer to the eHealth Help, Live Health.

15. Click OK to modify the response path elements and close the Modify Path Elements dialog.

16. Click Close on the Path/PVC Manager dialog.

17. Click OK or Apply in the Poller Configuration dialog to save the changes.

---

### Modify Source and Destination Elements

You can modify a response source or destination element by changing its name, alias name, IP address, or community string.
Since eHealth does not poll response sources and response destinations, the Poll field in the Poller Configuration dialog is not active. When you view response elements, N/A appears in the Poll field.

**To modify a source or destination element**

2. Select an element in the Poller Configuration dialog.
3. Click Modify. The Modify Element dialog appears.
4. Do one or more of the following:
   - Change the element name or alias name.
   - Specify another IP address.
   - Change the community string and read community string for a response source element.
   - Change the discovered information (system name and interface).
5. Do one of the following:
   - Click Apply/Next to update the element with the changes and display the next element in the poller configuration list.
   - Click OK to update the element with the changes and close the Modify Element dialog.
6. Click OK or Apply in the Poller Configuration dialog to save the modifications to the elements.

**Delete Response Elements**

You can use the Poller Configuration dialog to delete Cisco IP SLA and Juniper RPM response source and destination elements. You delete these types of response elements using the Path/PVC Manager dialog.

**To delete response source or destination elements**

2. Select one or more elements in the Poller Configuration dialog and click Delete. If you delete a source or a destination, you also delete all paths associated with that element.
   
   **Note:** For more information about deleting elements, see the *eHealth Administration Guide*.
3. You must click OK or Apply in the Poller Configuration dialog to save the information that you change.

**Important!** If you click Cancel in the Poller Configuration dialog, you will lose all work you have performed since you opened this dialog.
To delete response path elements

2. In the Poller Configuration dialog, click Path/PVC Manager. The Path/PVC Manager dialog appears.
   Note: The title of the Path Manager dialog indicates the Set Element Filter setting in the Options dialog. If you have not set a filter, the title indicates that the Path Manager dialog lists all paths. If you have set a filter, the title indicates the group name.
3. Select one or more elements, and click Delete.
4. Click Close on the Path/PVC Manager dialog.
5. Click OK or Apply in the Poller Configuration dialog to save the information that you changed.
Chapter 6: Manage Response Using eHealth Reports

This chapter provides an overview of the types of eHealth reports that you can run to display response data, and describes how to configure and run those reports to manage the response elements in your configuration.

It includes the following sections:
- Overview of Response Reports
- Prepare to Run Response Reports
- Run Response Reports

Overview of Response Reports

Using eHealth Response, you can report on response sources, destinations, and paths. You can run the following standard and licensed eHealth reports to display your response element data:
- At-a-Glance
- Top N
- Trend
- Health
- Service Level
- MyHealth
- What-If

Note: When you generate a Trend report for a response element, you can report on the total number of transactions collected by an AR agent that exceed a given time constraint defined in an Application rule for that element.

Many reports show the breakdown of response time into client, network, and server time. This breakdown identifies the part of your infrastructure to investigate for the source of a response time problem. The information helps you identify and correct problems quickly, minimizing their impact on productivity.
Run the special set of reports described in the following table to provide you with the information you need to manage the response time and performance of applications in your infrastructure.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level</td>
<td>CIO Executive</td>
<td>This report shows response time and related metrics for all applications for all groups, or for a selected group list. Use this report to summarize current service levels experienced by user groups.</td>
</tr>
<tr>
<td>Health</td>
<td>Path Summary</td>
<td>This report presents the poorest performing paths in a selected group. It breaks down performance by component—client, network, server—so you can troubleshoot the component that is the major source of the problem.</td>
</tr>
<tr>
<td>At-a-Glance</td>
<td>Application Response Client Set</td>
<td>This report helps the network operations center (NOC) analyst or planner diagnose application performance in detail. It shows response time and related metrics for all applications used by a selected client set.</td>
</tr>
<tr>
<td></td>
<td>Application Response Service</td>
<td>This report provides more detail on application performance for the NOC analyst or planner. This report shows response time and related metrics for all client sets served by a selected application service for a particular application.</td>
</tr>
<tr>
<td>AdvantEDGE</td>
<td>Service Availability</td>
<td>This report monitors the response time and availability of critical network services from any system within the enterprise network. Service Availability performs real test transactions using a specified service to provide a real view of the response times and availability for common network services.</td>
</tr>
<tr>
<td>AdvantEDGE</td>
<td>VQM</td>
<td>This report monitors the mean opinion score (MOS) for response paths between two systems.</td>
</tr>
<tr>
<td>At-a-Glance</td>
<td>VQM</td>
<td>This report provides important performance indicators for a specific VQM response path element during the report period.</td>
</tr>
</tbody>
</table>
Prepare to Run Response Reports

Before you run reports on response elements, as a best practice complete the following prerequisite tasks:

- Create response groups and group lists to organize your elements, as described in the eHealth Administration Guide.
- Set response limits to measure the performance of a response path element.
- Create any service profiles that you want to use, as described in the eHealth Administration Guide.

Note: You can run Top N, Trend, and Health reports on groups, and you can run Service Level reports on groups or group lists. You can use Live Exceptions to monitor both groups and group lists. To generate Health and Service Level reports, you must obtain the appropriate eHealth licenses.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level</td>
<td>Application Response:</td>
<td>These reports determine the relative performance of an application for a specific location or functional group, or for a group of locations or functional groups for selected applications. You can use them to report on the applications, modules, and module sets within your infrastructure.</td>
</tr>
<tr>
<td></td>
<td>- Service Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Service Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Service Performance</td>
<td></td>
</tr>
<tr>
<td>VoIP:</td>
<td>Executive</td>
<td>VoIP Executive reports provide information about the availability, usability, usage, and usage trends of the VoIP service. They can also help you to determine which customers are receiving poor service and how you can fix it.</td>
</tr>
<tr>
<td></td>
<td>- IT Manager</td>
<td>VoIP IT Manager reports provide information about long-term trends in voice quality, as well as volume trends within the VoIP infrastructure. They can help you determine whether the current infrastructure is providing adequate service and how it will grow.</td>
</tr>
<tr>
<td></td>
<td>- Service Customer</td>
<td>VoIP Service Customer reports provide information about whether service customers are getting good service, including information about the availability and quality of the VoIP service, the amount of the service that they are using, and their usage trends.</td>
</tr>
<tr>
<td></td>
<td>Response Executive</td>
<td>These reports provide information about the response times, failed attempts, and health of the response elements in your region, department, or business process. You can run them for response paths, endpoints, and client sets, setting service level ranges to analyze data based on your service goals and agreements.</td>
</tr>
<tr>
<td></td>
<td>- Response Service Customer</td>
<td></td>
</tr>
</tbody>
</table>
Response Groups and Group Lists

**Note:** For procedures to create groups and group lists, see the *eHealth Administration Guide*.

*eHealth* enables you to organize your elements into groups so that you can associate related elements, such as those for a specific department or customer, and generate reports for those specific element sets. To organize your groups, you create group lists.

For example, you can use group lists to model larger organizations, such as all of the groups for a customer, a company, geographic region, and so on. By focusing on a subset of elements—rather than all elements in your infrastructure—you can create effective reports that address your specific needs. A group can belong to multiple group lists. You can use groups and group lists to control access to reports and elements in the *eHealth* Web user interface.

**Note:** To organize Application Response elements, you create agent sets through the Application Response interface. These agent sets appear as groups in *eHealth*.

A group of response elements can contain response endpoints (sources and destinations), paths, or both. Group lists can contain response groups.

**Response Element Groups - Guidelines**

**Groups**

A collection of monitored elements. Typically, groups organize elements by geographic location, department, market segment, or vendor.

When you create response element groups, use the following guidelines:

- You may want to create the following types of groups:
  - All VQM paths that originate from the same transmitter/receiver.
  - All Cisco IP SLA paths that originate from the same Cisco device.
  - All Juniper RPM paths that originate from the same Juniper router.
  - All paths that test the same protocol.
- Select one of the following element types under Available Elements:
  - Response Client Set
  - Response Source
  - Response Destination
  - Response Path

  **Note:** The list shows the available elements for the type that you select.

- When creating groups of router/switch elements, LAN/WAN elements that correspond to groups of response charts, or response elements, the *eHealth* administrator must use the *same* name as the response path group name; otherwise, the user cannot successfully drill down to Top N reports from Service Availability and Application Response Path Summary reports.
Response Group Lists - Guidelines

Group List

A group list is a collection of one or more groups. Group lists allow you to associate related groups.

When you create response element group lists, use the following guidelines:

- You may want to create the following types of group lists:
  - A response group list of all of your VQM groups.
  - A multi-tech group list of all of your response path groups.
  - A response group list of all of your response groups.

- To create a new Response group list, you can use the Group List, Run Report, and Schedule Report dialogs, which are all accessible from the eHealth console.

Response Limits

Response Limit

A response limit is a time threshold (specified in milliseconds) used to measure the performance of a response path element. When the response time for a path exceeds the limit, the path is not meeting the desired response time performance.

You set the response limit for each path element to measure performance based on its characteristics and the needs of the users or applications. For example, a path that uses long-distance WAN links might have a very high response limit because traffic typically takes a long time to travel over that link. However, paths that use high-speed LAN links to connect your sales department workstations to the sales application server might have very low response limits because delays could impact sales order processing.

You can group related response path elements to monitor and report on them. For example, you can monitor a group of response path elements using Live Health so that you will be notified when a path in the group exceeds its response limit or matches the alarm rule criteria. If you have the optional Health report license, you can run a report for a group of path elements (that could each have different response limits) to locate paths that exceeded their limits during the report period and to determine whether the response time over those paths is improving or degrading.
Evaluate and Set Response Limits

eHealth provides two commands that evaluate and set response limits for your response path elements:

nhGetRespLimit

The nhGetRespLimit command evaluates and recommends response limit values for a group of Cisco IP SLA or Juniper RPM response path elements. It uses a Top N report to calculate the average response time for the group over a specified time period. The command also recommends a response time limit value based on the average multiplied by a limit factor.

nhSetRespLimit

The nhSetRespLimit command sets the response limits based on an input file such as the nhRecommend.txt file that is produced by nhGetRespLimit.

To run the nhGetRespLimit command

1. Log on to the eHealth system as the eHealth administrator.
2. Change to the eHealth directory by entering the following command in any terminal window (such as an xterm or shell window):
   
   ```bash
cd /ehealth
   ehealth
   ```
   
   Represents the full pathname of that directory.
3. Enter the following command:
   
   ```bash
   ./bin/nhGetRespLimit
   ```
4. At the following prompt, enter the name of a group of response path elements:
   
   Enter a response path group name:
5. At the following prompt, enter the time range over which you want to evaluate the average response time:
   
   Time range:
   
   1) Custom
   2) Today
   3) Yesterday
   4) This week
   5) Last week
   6) This month
   7) Last month
   8) Previous hour
   9) Previous 12 hrs
   10) Previous 24 hrs
   11) Previous 7 days
   12) Previous 4 hrs
   What is your choice? (1-12)
6. At the following prompt, enter the factor that eHealth uses to determine the recommended response time limit:
   
   Enter a limit factor [2.0]
   
   You can use the limit factor to tailor the recommended response time limit based on a multiple of the average response time. The default value is 2.0, which causes the script to recommend a limit value that is twice the average response time.
The command then displays the information that you entered and prompts you for the next step. The following is a sample output:

You have specified the following parameters:

Response path group name: PathGrp
Time range: today
Start Date/time: 
End Date/time: 
Limit factor: 2.0

At this point, you can:
1) Continue with retrieval of response limit
2) Change response path group name
3) Change time range
4) Change start date/time
5) Change end date/time
6) Change limit factor
7) View the parameters entered
8) Exit the Script

What is your choice? (1|2|3|4|5|6|7|8)

7. Change the parameters that you specified, or enter 1 to continue. If you enter 1, the command displays the following:

Getting response path limits...
Creating recommendation file: /ehealth/output/topN/nhRecommend.txt

At this point, you can:
1) Exit the script and view/edit the response path limit recommendation in a text editor.
2) View the recommendation

What is your choice? (1|2)

8. Do one of the following:
- Enter 1 to exit the script and review the recommendations file, /ehealth/output/topN/nhRecommend.txt.
- Enter 2 to display the nhRecommend.txt file contents.

The following is a sample nhRecommend.txt file:

Output of the Average Response with Recommended Limit:
<table>
<thead>
<tr>
<th>Element</th>
<th>Avg Response</th>
<th>Recommended Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;path1-UDP&quot;</td>
<td>25.00</td>
<td>50.00</td>
</tr>
<tr>
<td>&quot;path2-ICMP&quot;</td>
<td>25.00</td>
<td>50.00</td>
</tr>
</tbody>
</table>

At this point, you can:
1) Exit the script and view/edit the response path limit recommendation in a text editor.
2) Launch the Set Response Limit script (nhSetRespLimit).

9. Do one of the following:
- Enter 1 to exit the script.
- Enter 2 to run the nhSetRespLimit command.
To run the nhSetRespLimit command

**Note:** If you have already run the command through the nhGetRespLimit command (as described in the previous section), proceed to Step 4.

1. Log on to the eHealth system as the eHealth administrator; then change to the eHealth directory by entering the following command in any terminal window (such as an xterm or shell window), where `ehealth` is the full pathname of that directory:
   
   ```
   cd /ehealth
   ```

2. Enter the following command:
   
   ```
   ./bin/nhSetRespLimit
   ```

3. Enter the name of a recommendation file:
   
   ```
   Enter a recommendation file name: [/ehealth/output/topN/nhRecommend.txt]
   ```

   **Note:** If you specify a file other than `nhRecommend.txt`, confirm that it uses the following format for each response path element. The *average* and *recommended* values should be in the format `nn.nn`; for example: 25.00, 35.60, and so on.

   ```
   "elementName" average recommended
   ```

   The system displays the following information:

   ```
   You have specified the following parameter:
   Recommendation file name: nhRecommend.txt
   ```

   At this point you can:
   
   1) Continue and set the response limits
   2) Change the recommendation file
   3) Quit

   What is your choice? (1|2|3)

4. Do one of the following:

   - Enter 1 to update the response path elements to use the recommended value as the response limit (which you can view using the Modify Path Element dialog).
   - Enter 2 to specify a different recommendation file.
   - Enter 3 to exit the command without changing the response limits.

---

**Run Response Reports**

You run reports on response elements from the eHealth console and Web user interface. Health and Service Level reports require separate licenses and work slightly different from other report types. The following sections describe these report types.

**Note:** You can also run At-a-Glance and Trend reports from One Click for eHealth.

This section describes running the following types of reports:
Run Response Reports

- At-a-Glance reports
- Trend reports
- Service Level reports
- Health reports
- Response Path Summary reports

At-a-Glance Reports

At-a-Glance reports provide an overall look at the critical performance indicators for a response element. Each At-a-Glance report presents several charts on a single page, allowing you to easily compare variables to troubleshoot performance problems. When you identify a problem, you can then drill down directly to a Trend report for more details.

You can run At-a-Glance and Trend reports on performance variables such as round-trip delay, jitter, and jitter variation to obtain an accurate view of the quality of response time or VoIP service that a user experiences.

The following graphic shows sample charts from an At-a-Glance report for a Juniper RPM response path. These charts show metrics for jitter that you can use to monitor and manage attributes of network traffic that affect the quality of voice service.
Trend Reports

Trend reports show a historical view of response performance. Trend reports are useful for troubleshooting response elements by revealing patterns over time, as well as relationships between multiple response elements or multiple variables.

You can use a Trend report to plot one variable for up to ten elements over any time period, or to plot up to ten variables for one element. You can also run a group Trend report that shows either of the following:

- Aggregate data for a group of elements, which allows you to identify trends for the group as a whole
- A separate chart (for each of the chosen variables) for each element in a group, which allows you to compare the performance of elements within a group

The following graphic shows a sample Cisco IOS IP SLA Trend report. The report shows that, for the specified time period, average response time to ping devices from the router was fairly steady, except for a spike of response time between 2:20 P.M. and 2:50 P.M; this situation may merit further investigation.

Service Level Reports

If you have a Service Level Report license, you can run Service Level reports to on response elements to accomplish the following:

- Determine relative performance of applications within your infrastructure.
- Determine the availability, usability, usage, and usage trends of the VoIP service and long-term trends in voice quality.
- Obtain monthly or quarterly summary information about an enterprise, a region, a department, or a business process.
Before you run these reports, create groups and group lists for your response elements. You might prefer to specify the ranges against which to measure service levels. eHealth uses a default service profile that defines values from these ranges, but you might prefer to create your own customized service profiles.

**Note:** For more information about running standard eHealth reports for response elements, see the eHealth Help.

### Health Reports

If you have a Health report license, you can run a Health report on the response paths or response endpoints (sources and destinations), depending on the elements that appear in the Exceptions section and in the Situations to Watch table. That is, a report on paths and a report on endpoints in the same group are identical. However, a Health report on paths contains only paths in the Exceptions section and in the Situations to Watch table, whereas a report on endpoints contains only endpoints in the Exceptions section and in the Situations to Watch table. In either case, the data in the report pertains to the paths in the group.

For a response path Health report, eHealth includes the paths listed in the group. For a response endpoint Health report, it includes all paths whose source or destination is an endpoint in the group. A Health report on endpoints could result in duplicate path data if an endpoint and a destination are in the group.

### Health Report Sections

Health reports on response elements contain following four sections:

**Note:** The standard response Health report is designed for Service Availability, Cisco IP SLA, and Juniper RPM. For Application Response, use the CIO Summary report.

#### Exceptions Section

The Exceptions section of a daily Health report contains an Exceptions Summary and an Exceptions Detail report. Examine this section to determine if an element experienced high latency, high packet drops, long response times, or low availability during the report period. The Exceptions Summary report lists those elements that experience the highest rate of these conditions. The Exceptions Detail report also provides details about the most frequently occurring of these conditions.
Summary and Top Ten Section
The Summary and Top Ten section contains summary information on the elements in the report and on the response time leaders and change leaders. The charts in this section report on the average normalized response time for all elements by day and by hour, the top ten leaders in response time, and the top ten change leaders in response time. It also contains a Situations to Watch chart that lists either the endpoints or paths that require close monitoring.

Element Detail Section
The Element Detail section compares data for each element in the report. This section provides charts that show the Health Index, response time compared to the baseline, response time compared to limit, and availability of each element.

Supplemental Section
The Supplemental section provides more detail on the group. Some of the charts in this section allow you to view the same information displayed in the Summary and Top Ten sections, but for more elements than the other sections provide.

Other charts in the Supplemental section do the following:
- List the threshold settings for Health Indexes and Situations to Watch.
- List elements that experienced missed polls, bad polls, and reboots.
- Display the availability, response, and reachability of each element in the report.

Response Path Summary Reports
You can determine which paths in a selected group have the worst performance by generating response path Daily Summary Reports. For Cisco IP SLA, Juniper RPM, and Service Availability, you can report on path performance by component (specifically, DNS lookup, TCP connect, and transaction time). For Application Response, you can report on path performance by client, server, and network.

The Daily Summary Report charts provide the following information:
- Ranking of the 25 response paths with the worst performance, according to their average response time
- Total response time for each group for each unit in the baseline period compared to the overall trend for the group
- Summary of each component’s contribution to the total response time for the selected report period
Generate the Report

To generate a response path summary report, select the specific report type from the Report list in the Run Health Report dialog as follows:

- To report on a SystemEDGE agent with the Service Availability module, select ServiceResponse.
- To report on an Application Response agent, select ApplicationResponse.

After specifying the report type, select ResponsePath from the Subject list; then select a group from the Group list.

**Note:** When creating groups of router/switch elements, LAN/WAN elements that correspond to groups of response charts, or response elements, the eHealth administrator must use the same name as the response path group name; otherwise, the user cannot successfully drill down to Top N reports from Service Availability and Application Response Path Summary reports.

**Note:** For complete instructions, see the procedure on running Health reports in the *Reports User and Administration Guide*.

Configure Live Health to Notify You of Problems

Live Health can notify you of potential delays, failures, and other problems that occur with your applications. When you configure Live Health for Application Response, you establish levels of alarms from normal to critical. Application Response automatically notifies you through a Live Status diagram when application performance begins to degrade.

Initially, use the Live Exceptions default profiles to monitor your response data. After you accumulate data over time, create new profile associations for your response elements. Use the Live Exceptions Browser to configure the profiles for the response elements that you want to monitor.

**To associate the default Live Exceptions profiles to your Response groups**

1. Open a Live Exceptions Browser.
3. Click New. The Setup Subjects Editor dialog appears.
4. Under Subject Type, select Groups.
5. From the Subjects list, select the group list that you created.
6. From the Profiles list, select all Response profiles listed.
7. Click OK.
Configure Live Health to Notify You of Problems

eHealth begins to monitor your response elements using the default profiles. However, the profiles may not be well-suited to your environment. To ensure that Live Health is working, you should create a custom profile with one rule to test.

**To create a new (custom) Live Health profile and associate it to your Response groups**

1. Open a Live Exceptions browser.
2. Select Setup, Profiles. The Profiles Manager dialog appears.
3. Click New Profile.
4. In the Create Profile dialog, specify a name such as MY_AR_TEST_PROFILE; then click OK.
5. Click New Rule.
6. Under Element Type, select Generic Response Path Set.
8. Specify a rule message such as Test rule for transactions.
9. Next to Time, specify 1 in each field.
10. Under Variable, select Transaction Timeouts.
11. Under Condition Type, select Time Over Threshold.
12. Select Above and specify 1 in the Percent field.
13. Click OK; then click OK in the Profiles Manager dialog.
14. When the Information dialog appears, click OK to confirm that Live Health should send the data to the server.
15. Associate the new profile to Response groups as follows:
   b. Click New. The Setup Subjects Editor dialog appears.
   c. Under Subjects, select Group Lists.
16. From the Subjects list, select the response group lists to which you want to associate the profile.
17. From the Profiles list, select the profile that you just created.
18. Under Calendars, accept the default.
19. Click OK in the Setup Subjects Editor dialog.
20. Click OK in the message that indicates that your message has been sent to the server.
21. Click OK in the Setup Subjects Editor dialog; then click OK in the message box that indicates Live Health has send your message to the server.

**To create a Live Status application view of your clients sets**

1. Run Live Status; Select Start, Programs, eHealth, Live Status.
2. In the Live Status window, select File, New Diagram.
3. In the New Diagram dialog, specify a title for the application view in the Title field.

4. Under Group Lists, select your Response group list.

5. Click OK. The Live Status window refreshes and then displays a diagram similar to the following. You can right-click on any group member to generate a report on it.
eHealth Application Response can monitor applications published to Citrix® Metaframe®. Due to the multi-tier nature of Citrix, the process for configuring Application Response to monitor these applications is different from the process for typical client/server applications. This appendix describes concepts that are unique to an Application Response implementation for Citrix and provides instructions for configuring Application Response to monitor Citrix applications.

This topic is organized into two main sections:
- Application Response in a Citrix Environment describes important concepts.
- Configure Application Response provides procedures for setting up Application Response to monitor Citrix applications.

Read the entire document before beginning the configuration process. If you have any questions or issues, contact CA Technical Support.

**Application Response in a Citrix Environment**

In a Citrix environment, an end user uses a published application within a Citrix client session on an end-user device, such as a PC or a thin-client network device. The Citrix client sends the mouse clicks and keystrokes to the Citrix server, where the application client resides. The application client processes the user input and sends requests to the application server, which communicates with a database server or other back-end servers. Replies from the application server follow the reverse path. The following graphic illustrates a Citrix environment:
Measure Response Time

In a Citrix environment, you install an Application Response (AR) agent on each Citrix server. When a user uses a monitored application, Application Response measures total response time, which consists of the following components:

**Client time**
Processing time for the application client, which resides on the Citrix server.

**Network time**
The combined total of $N_1$ network time (between the Citrix client and the Citrix server) and $N_2$ network time (between the Citrix server and the application server).

**Server time**
Processing time for the application server, which includes processing time for any back-end servers, such as database servers.
Application Response does not include client think time, which occurs on the end-user device, in its calculation for total response time. In general, the Citrix client performs screen emulation quickly, so any delays on the end-user device are usually negligible. Also, to include this small amount of client think time in total response time, you would need to install and maintain the AR agent on every end-user device, which could be very labor-intensive and costly. By placing AR agents on the Citrix servers, you are able to get the response time data that you need more efficiently and at a lower cost.

User Access to Your Citrix Applications

In some Citrix environments, each end user accesses applications from a single device, and only that user uses the device. In an office, for example, employees use PCs at their desks to access published applications to perform work, and they do not generally share PCs with other employees.

In other environments, end-user devices are shared among several users. In a hospital, for example, kiosks may provide employees who do not have offices, such as nurses and janitorial staff, with access to published applications. In this case, any employee can use any available kiosk to perform work.

The type of user access for your Citrix environment may influence how you use Application Response to track end-user response times, as described in the next section.

AR Response Paths for Citrix Applications

When an end user uses an application, the AR agent collects response time data and, at every heartbeat (every five minutes by default), sends aggregated data to the AR controller, which then forwards the data to the eHealth server and database. When the data reaches the eHealth server, eHealth creates an AR response path if one does not already exist.

By default, a response path for Application Response uses the following format:

\[clientName-application-module-server-AP\]

- **clientName**: The hostname of the end-user device.
- **application**: The name of the application.
- **module**: The name of the transaction being performed.
- **server**: The name of the application server to which the application connected.
- **AP**: Indicates an Application Path.
For example, if Bill is using the Yellow system to perform the Create Purchase Order transaction with SAP, which connects to SAPserver3, the response path is yellow-SAP-CreatePO-SAPserver3-AP

Application Response does not include the Citrix server name in the response path.

**Client Names or User Names in Paths**

With the client name in the response path (the default), you can easily trace performance problems to specific end-user devices. However, if several users typically share one device, this method does not provide user-specific performance data, which can be useful when analyzing the end-user experience.

As an alternative to client name, you can configure Application Response to use the username (terminal server login) in the response path instead. Using the previous example, the response path would be:

CITRIX1-bill-SAP-CreatePO-SAPserver3-AP

**CITRIX1**

The name of the Windows NT or Active Directory domain in which the Citrix server farm resides.

If several users typically share one system, this option allows you to track application usage by user instead of by end-user system. However, if a user moves from one place to another, using different end-user devices in your organization, this method can produce confusing results. For example, on system Orange Bill has fast response time, but on system Yellow he has slow response time. Regardless of which system he uses, however, all of Bill’s response time is aggregated for reporting purposes. For this reason, CA recommends that you track application activity by username only if users typically use the same systems to perform application activity.

More information:

Configure AR Paths to Include Usernames

**Trace Problems to Citrix Servers**

Response paths indicate the end-user device or user, the application, transaction or module, and application server involved. This information provides the end-to-end data that you need to understand the end-user experience. When troubleshooting performance problems, however, you may need to trace issues back to specific Citrix servers. While AR paths do not include the name of the Citrix server involved in application activity, you can trace performance problems to Citrix servers as follows.
Single Citrix Server

If you use a single Citrix server for an application or if you specify that particular Citrix clients always connect to specific Citrix servers, you can trace client-side problems to those Citrix servers based on the application or Citrix client indicated in the response path.

Load-Balanced Citrix Server Farm

If you use a Citrix server farm with a load balancer, the load balancer may direct a Citrix session to any one of several Citrix servers. Because response paths do not include the Citrix server name, Application Response cannot identify which Citrix server is involved in application activity.

When Application Response shows slow client response times (for the application client, where the Citrix server resides), you can run a System Health report for a group of Citrix servers to look for exceptions and situations to watch. If this report identifies problems with particular servers, you can then run At-a-Glance reports on those servers for more detailed information. These capabilities require that you install SystemEDGE agents on the Citrix servers. You can also use eHealth application insight modules (AIMs) for additional information about the performance of your Citrix servers.

Organize Response Elements for Citrix Applications

To report on the end-user experience for published applications, you can create eHealth groups and group lists for end-user devices or usernames, applications, specific transactions, and application servers. You create these groups by organizing the AR response paths, response sources (end-user devices or usernames), and response destinations (application servers). When you organize these response elements to reflect your application infrastructure, you can generate reports that provide many different views of the end-user experience and provide the details you need to identify and troubleshoot problems.

More information:

Step 4: Organize Response Elements

In a Citrix environment, however, you cannot use client sets for reporting purposes. Client sets are groups of AR agents. (You can use client sets to report on traditional client/server applications.) Because AR agents are installed on Citrix servers and Application Response does not track application activity by Citrix server, client sets are not useful in a Citrix environment. However, you can organize AR agents on Citrix servers into agent sets to simplify agent management.

For example, create Agent Set A for Citrix servers in one location and Agent Set B for Citrix servers in another location, and use these agent sets to start and stop agents on servers in each location.
Configure Application Response

Note: For information on creating agent sets, see the eHealth Help, Application Response.

Configure Application Response

The process for configuring Application Response to monitor Citrix applications is as follows:
1. Install AR agents on Citrix servers.
2. Define Citrix-specific settings.
3. Configure the target application.
4. Organize response elements for reporting.
5. Configure Live Health.

Procedures for each step follow. These procedures assume that you have installed and configured eHealth as described in the eHealth Installation Guide. They also assume that you have a working knowledge of Citrix applications and terminology and know how to use eHealth to perform administrative functions.

Note: If your Citrix implementation includes more than 1,000 users or 20 Citrix servers in a single server farm (or both), you may need to perform additional configuration steps. Before you start, contact your CA Sales Engineer or Technical Support for help in planning your Application Response implementation for Citrix applications.

Step 1: Install AR Agents on Citrix Servers

You must install one AR agent on each Citrix server that hosts the application clients to monitor. Installing AR agents involves the following steps:
   a. Enter AR agent licenses.
   b. Publish an AR agent installation program.
   c. Install the AR agent on each Citrix server.
   d. Confirm successful agent installations.

Step 1A: Enter AR Agent Licenses

For Application Response Terminal Server (TS) agent licenses for your Citrix servers, enter your license keys into the license.dat file. For instructions on entering licenses, see the eHealth Help, Administration.
Configure Application Response

Step 1B: Publish an AR Agent Installation Program

The AR Agent Publisher allows you to define settings for the AR agent that you will install on the Citrix servers. Use it to create an agent installation program. Download the Agent Publisher from the Application Response Web interface.

To create the AR agent installation program

2. Click Run. The Welcome dialog appears.
3. Select Generate an AR Agent Installation Program; then click Next.
4. Read the Software License Agreement, if it appears. If you accept the terms, click Yes to continue.
5. In the Edit Controller Information dialog, enter the name of the eHealth system in the Hostname field (that is, the host name of the system on which eHealth resides) and accept the default values in the Port and Agent Port fields; then click Next.

   Note: For the initial deployment, leave the Name field under Agent Set blank. When you install additional agents and set up grouping, use this field to associate agents with groups.

6. In the Options for Agent Install dialog, deselect Silent Agent Install, accept the other default selections, and click Next.
7. In the Agent Extensions dialog, click Next. After you deploy your test agent, you can return to the Agent Publisher and create a version of the agent that monitors Java applications and applets.
8. In the Enter Target Directory for Agent Install dialog, leave the field blank and click Next. By default, the program installs the agent on the boot drive of the Citrix server and creates an ehealth/agent/response directory.
9. In the Choose Destination Location and Program Name dialog, accept the default name and location or specify new values; then click Next.
10. In the Edit Agent Host Names dialog, click Next.
11. In the Start Generating Program dialog, review the information. If you want to change your settings, use the Back button.
12. When you are satisfied with the settings, click Finish.

The AR Agent Publisher creates a file named ARInstl.exe in the C:\ehealth directory (if you used the default settings). Now you can use this installation program to install the AR agent on the target Citrix servers.

Step 1C: Install the AR Agent on Each Server

Install the agent on each of the target Citrix servers, as described in the following procedure. The installation of the AR agent requires a system reboot, so perform this step when you can take the Citrix servers offline.
**Important!** *Do not* install the AR agent on Citrix servers by executing the AR agent installation program directly. Instead, use the Windows Add/Remove Program utility. This method avoids problems with security and registry settings on terminal servers.

**To install the AR agent on Citrix servers**

1. Deploy the AR agent installation program to the Citrix servers. You can do this using any method that is practical for your infrastructure, such as the following:
   - **Network**: Move the AR agent installation program to a network location that is accessible to all target Citrix servers, such as a mapped drive.
   - **Email**: Create an email message, attach the AR agent installation program to it, and mail it to a user account on each Citrix server. On each server, open the mail message and save the file in a temporary directory.

2. On each Citrix server, install the AR agent using the Windows Add/Remove Programs utility, as follows:
   a. Close any open programs.
   b. From the Windows desktop, select Start, Settings, Control Panel.
   c. Double-click Add/Remove Programs.
   d. Click Add New Programs.
   e. Click CD.
   f. In the Insert Program from CD dialog, click Next.
   g. In the Run Installation Program dialog, click Browse and navigate to the location of the AR agent installation program, ARInstl.exe.
   h. Click Finish.
   i. In the AR Agent Setup Complete dialog, click OK.

3. Reboot each Citrix server.

**Step 1D: Confirm Successful Agent Installations**

After installing the AR agent on all target Citrix servers, confirm that the agents were installed successfully and are communicating with the AR controller on the eHealth system using the following procedure.

**To confirm successful AR agent installations**

1. Access the Agent List page of the eHealth Web user interface, as follows:
   a. In a Web browser, log in to the eHealth Web user interface.

2. In the agent list, check the following:
   - The Name column lists the Citrix servers on which you installed AR agents.
Configure Application Response

- The State column displays On, indicating that the AR agent on each Citrix server is turned on and can monitor applications.
- The Status column shows a green circle, indicating that the AR agent is functioning normally on each Citrix server.
- The Licensed column shows a checkmark, indicating that the agent has a license.
- The Agent Type column displays TS, indicating that the agent is a terminal services agent.

More information:
If any of these columns do not show the appropriate settings, see Troubleshooting Tips.

Step 2: Define Citrix-Specific Settings

To configure Application Response to monitor Citrix applications, define the following settings:

- **Grant permission to create global objects.** Give Citrix users permission to create global objects.
- **If you use scripts to start published applications,** define the ApplicationPrograms registry setting to identify the application executables that Application Response is to monitor.
- **If you want to AR paths to specify the username** instead of the client name, you must define a setting on the eHealth system.

More information:

Grant Permission to Create Global Objects
Specify Executables for Published Applications
Configure AR Paths to Include Usernames

Grant Permission to Create Global Objects

The Windows domain administrator must give users permission to create global objects. This ensures that Citrix user sessions are able to load the DLLs required for application monitoring. You can do this by assigning these permissions to individual users, to existing user groups, or to a new group created specifically for users whose activity will be monitored using Application Response.

The following procedure describes how to grant permission to create global objects to an existing user group. Use these instructions or a similar procedure to help ensure that your Citrix users can create global objects.
**To grant permission to create global objects**

1. On a Windows domain server (or a Citrix server), select Start, Settings, Control Panel.
2. Double-click Administrative Tools.
4. Expand Local Policies and click User Rights Assignment.
5. Double-click Create global objects.
6. Click Add.
7. In the list of groups that appears, select a user group to which Citrix client users belong, such as Guest.
8. Click Add.
9. The selected group appears in the lower panel as `citrixServerName\groupName` (for example, Citrix1\Guest).
10. Click OK.
11. The new group is listed on the Local Security Policies Setting window.
12. Click OK.

**Specify Executables for Published Applications**

On a Citrix server, the AR agent creates an ARWatch process for each Citrix client session to monitor application executables. When an executable terminates, the AR agent stops monitoring its response time. In some Citrix environments, an initialization script or other program starts a published application. In this case, ARWatch may assume that, because the initialization script is terminating, the Citrix client session or application is also terminating. As a result, the AR agent stops monitoring response time for the application prematurely.

To avoid this problem, define the ApplicationPrograms registry setting to specify the executables that the AR agent is to monitor. This setting is a string value that specifies a comma-separated list of executable names (without the .exe file type extension). If the application uses a central process that runs the entire time, you can list that executable alone; if the application uses several processes that start and terminate within a session, you must list all of the executables.

You must define the ApplicationPrograms registry setting on each AR agent system (Citrix server). To simplify this process, you can use the eHealth Web user interface, as described in the following procedure.

**To define the ApplicationPrograms registry setting**

1. From the Systems & Apps tab of the eHealth Web user interface, click Agents, and then name of an agent system.
2. In the Agent Properties dialog, click Configure Agent.
3. In the New Custom Setting area, do the following:
   a. In the Name field, enter the following:
      ApplicationPrograms
   b. For Type, select String.
   c. In the Value field, enter the names of the executables to monitor without
      the exe file type extension, separated by commas.
      For example, to monitor Internet Explorer (IEXPLORE.EXE) and
      Microsoft Outlook (OUTLOOK.EXE), enter the following:
      IEXPLORE,OUTLOOK
   d. Click Insert.
   e. At the Insert the following Custom Value? prompt, check the information
      and click OK.
      The ApplicationPrograms setting appears in the Value field of the
      Existing Custom Settings area.
4. Click the Apply button that appears between the OK and Cancel buttons.
   eHealth immediately defines the registry setting on the AR agent system
   (within 30 seconds).
5. Repeat Steps 1 through 4 for each remaining AR agent system (Citrix
   server).

   If you need to modify the ApplicationPrograms setting later, for example, to add
   more executable names, return to the Agent Properties - Configuration dialog
   and, in the Existing Custom Settings area, select ApplicationPrograms from the
   Name list. Modify the value and click Apply.

Configure AR Paths to Include Usernames

By default, Application Response includes the hostname of the end-user device
in response paths for Citrix applications. If you want Application Response to use
the user name (terminal server login) in the response path instead, you must
define a setting on the eHealth system.

To understand the advantages and disadvantages of this setting, see Client
Names or User Names in Paths.

To include usernames in AR paths

1. On the Systems & Apps page, under Application Response, click Advanced
   Settings.
2. Under General, select the Use Client User Names for AR Agents in Terminal
   Server Mode check box.
3. Click Save Changes.

During the next agent heartbeat, Application Response propagates this setting
to all AR agents on Citrix servers.
Step 3: Configure the Target Application

Enable the application that you want to monitor. This process involves the following steps:

a. Enable the application.

b. Enable the application servers.

c. Run a test report.

More information:

Configure Application Performance Using Application Response

Manage Response Using eHealth Reports

In those sections, skip instructions for the following:

- Deploying AR agents. You have already completed this step.
- Using transaction logging to test agents with the Agent Transaction Viewer (ATV). Because the AR agent resides on a Citrix server, it can be difficult to use the ATV successfully unless you can specify the Citrix server to which a Citrix client will connect.
- Organizing deployed agents into client sets for reporting purposes. As explained in Organize Response Elements for Citrix Applications, you cannot use client sets to report on Citrix-published applications.

As a best practice, add one Citrix application to Application Response at a time, resolving any issues with that application before adding another application.

Step 4: Organize Response Elements

When Application Response is actively monitoring response times for published applications, create groups and group lists to organize AR elements for reporting purposes. You can also define response limits to set performance thresholds.

AR response paths are created in eHealth when users use applications. That is, a response path (from the end user to the application and module to the server) is not created until the user performs application activity. Therefore, you can create groups and group lists only after users have been using the applications and eHealth has created corresponding response paths, sources, and destinations.

To check whether paths have been created

1. In the eHealth console, select Reports, Edit Groups, Response Groups.
2. Click Add.
3. In the Add Response Groups dialog under Available Elements, select Response Path.
   The list in the right side of the screen displays existing response paths.
After AR response paths have been created, create the following groups:

- **Application servers**: Create a response group containing all servers for an application by using Response Destination elements (with the element names server-RD). If you have application servers in multiple locations, create a group for each set of servers in each location.

- **Regional or functional application users**: Create response groups for all users of an application in each location (for example, all SAP users in the Boston office [BostonSAP] and all SAP users in the Chicago office [ChicagoSAP]) using Response Source elements (with the element names clientName-RS or username-RS). If desired, you can also create response groups for application users who perform specific functions (for example, bank tellers and loan officers).

- **Transactions**: Create response groups representing individual transactions. To do this, filter Response Path elements by application and module name.

- **Citrix servers**: Create a system group for all Citrix servers (where SystemEDGE agents reside) or, if you have Citrix servers in multiple locations, create a system group representing each location.

After creating response groups, you can also create group lists (sets of groups), such as the following:

- **All application users**: Create a response group list of all users of an application, combining regional and functional groups of application users.

- **All application servers**: Create a response group list of all servers for an application in all locations, combining regional groups of application servers.

- **All transactions for an application**: Create a response group list of all transactions for an application, combining transaction-based groups.

- **All Citrix servers**: Create a system group list of all Citrix servers, combining regional groups of Citrix servers.

- **Citrix infrastructure**: Create a multi-technology group list of all Citrix-related groups to monitor the end-to-end performance of Citrix applications from a single Live Status display.

**More information:**

AR Response Paths for Citrix Applications

Troubleshooting Tips

Manage Response Using eHealth Reports (to create Response Groups)
Step 5: Configure Live Health

If you use Live Health, you can configure it to notify you of performance problems with your Citrix applications. Initially, you can use the Live Exceptions default profiles to monitor your response data. Later, you can use historical response data to refine these thresholds and create new profile associations for your response elements. You use Live Exceptions to configure the profiles for the Citrix applications that you want to monitor in Live Health.

The process for configuring Live Health to monitor Citrix applications is the same as the process for traditional client/server applications.

**More information:**

Manage Response Using eHealth Reports

Troubleshooting Tips

Use the following methods to resolve issues when configuring Application Response to monitor Citrix applications. If these tips do not help you to solve the problems that you are experiencing, contact CA Technical Support.

**More information:**

Troubleshooting Application Response

Agents Do Not Appear in Agent List

**Symptom:**

Target Citrix servers on which you installed AR agents do not appear in the agent list.

**Solution 1:**

Wait a few more minutes and click Refresh Data. It can take up to 15 minutes for the AR agents to register with the eHealth server.

**Solution 2:**

Verify your web browser is set to update with every visit to a page.

**To verify Internet Explorer**

1. From the Web browser, select Tools, Internet Options.
2. In the Internet Options dialog, select the General tab; then click Settings under Temporary Internet Files.
3. In the Settings dialog, select Every visit to the page; then click OK.
4. Click OK to close the Internet Options dialog.
5. In the eHealth Agent List page, click Refresh Data.

The updated page should list the Citrix servers on which you installed AR agents.

**State Column Does Not Display “On”**

**Symptom:**

The State column of the agent list displays Off instead of On for an AR agent.

**Solution:**

Refresh the page display by restarting the agents.

**To restart agents**

1. In the agent list, select the check box to the left of the agent name.
2. Click Start Selected Agents.

After the screen refreshes, the State column should display On, and the Status column should show a green icon.

**Status Column Does Not Show Green**

**Symptom:**

If the Status column of the agent list does not show a green circle, it indicates that the AR controller is having trouble communicating with the AR agent on that system.

**Solution:**

On the agent system, use the Services dialog to confirm that the AR agent process (Application Response Agent Proxy) is started. If a red square appears with a “hook not loaded” message, you may need to grant users permission to create global objects.

**More information:**

Grant Permission to Create Global Objects

**License Column Does Not Display a CheckMark**

**Symptom:**

An AR agent license is not available.

**Solution:**

Confirm that you entered a sufficient number of AR terminal services agent licenses for the Citrix servers on which you installed the AR agent.
Agent Type Column of the Agent List Does Not Display TS

**Symptom:**
No AR TSAgent license has not been entered.

**Solution:**
Use the eHealth console to enter the appropriate number of AR TSAgent license keys (one for each Citrix server).

**Note:** For details, see the eHealth Help.

Sample Report Empty

**Symptom:**
The AR agent is not collecting data when a sample report is run to confirm the AR agent is working.

**Solution:**
Do one of the following:
- Grant users permission to create global objects.
- Define the ApplicationPrograms registry setting for the agent. If you have already defined this setting, check to make sure that it includes all application executables for the monitored applications. If ApplicationPrograms does not include a required executable, the AR agent may not recognize application activity. Also check to make sure that you did not include the exe file type extension with the executable names.
- If you still do not see report data, try the following:
  - Stop and start the agent.
  - Start transaction logging for the agent and use the Agent Transaction Viewer (ATV) to determine whether you can see application transaction data from the agent. For instructions, refer to the eHealth Help for the eHealth Web user interface.
  - Check ehealth/data/response/arcontrol.log on the eHealth system and look for error messages that indicate potential communication problems with the agent. For additional assistance, contact CA Technical Support.

**More information:**
Grant Permission to Create Global Objects
Specify Executables for Published Applications
AR Response Paths Do Not Appear

**Symptom:**

You checked whether AR response paths have been created and no paths appear in the list.

**Solution:**

Check the following:

- Are users using the monitored applications to perform tasks? AR response paths do not appear in the eHealth database until after those paths are exercised by users.
- Have you waited a sufficient amount of time after users performed application tasks? It can take 20 to 30 minutes from the time a user performs a task until eHealth creates a corresponding response path.

More Information

- For information about implementing Application Response to monitor applications, see the eHealth Help, Application Response.
- For instructions on how to customize Application Response to monitor transaction-specific response times, see the eHealth Help, BT Studio.
Appendix B: Troubleshooting Application Response

This appendix describes common error messages and problem symptoms, and provides solutions for the setup and operation of Application Response using default rule sets. It is organized in two sections:

This document is organized into the following sections:
- Guidelines
- Error Messages and Agent Conditions
- Common Symptoms

Guidelines

Use the following guidelines to help you troubleshoot Application Response.

- To help ensure that you are running Application Response with the latest fixes and enhancements, confirm your installation is at the following release and patch levels:
  - eHealth r6.0 SP4
  - eHealth r6.1

- If you encounter a problem and you know that you have applied the latest patch, look for related error messages in the product interface. If none exist, check the controller and agent log files.
  
  Find error messages on the eHealth system in the `ehealth\data\response\arcontrol.log` file, where `ehealth` is the full path to the directory in which you installed eHealth.
  
  Find error messages on each AR agent system in the `ar_agent\agent\response\aragent.log` file, where `ar_agent` is the full path to the directory in which you installed the AR agent.

- If you find an error message in the log files, scan the error messages. If you did not find a related error message in the logs or if the error message is not covered in this document, scan the list of common symptoms.

  If you do not find information about your problem in this focus topic, search the eHealth knowledgebase at the following web address:
Before you contact Technical Support, see Information to Collect for CA Technical Support.

Error Messages and Agent Conditions

This section describes solutions to problems that are associated with specific error messages and agent conditions. Find error messages in the following locations:

- On the eHealth system in the ehealth\data\response\arcontrol.log file and in the ehealth\log\system.log file, where ehealth is the full path to the directory in which you installed eHealth
- On each AR agent system in the ar_agent\agent\response\aragent.log file, where ar_agent is the full path to the directory in which you installed the AR agent

You can also find agent conditions on the eHealth system in the ehealth\data\response\agentcnd.log file.

Agent dying due to...

**Symptom:**

This type of error message indicates that the agent detects conditions that warrant it to stop and restart itself. Some transactions will be lost as a result but the agent will probably recover. A possible cause of this error is a poorly defined rule.

**Solution:**

When an AR agent stops, it stops collecting data. You or the application user must restart any monitored applications. Also, in a terminal services (Citrix Metaframe or Windows Terminal Server) environment, AR does not resume collecting data until each of the users logs out and logs in.

ARWatch Not Running

**Symptom:**

An AR agent has the ARWatch Not Running condition and AR is running in a traditional, single-client/server environment (not a terminal services environment).

**Solution:**

**Restart the ARAgent Proxy service on that system as follows:**

1. From the Windows desktop, right-click on the system icon.
2. Select Manage.
3. In the Computer Management dialog, select Services and Applications.
4. Select Services.
5. In the list of services, select Application Response Agent Proxy.
6. Click Start.
   If the process stops again, contact Technical Support.

If an AR agent has the ARWatch Not Running condition and AR is running in a terminal services environment, the ARWatch process may have ended prematurely because of a missing registry entry, or the entry may be missing the name of the application.

**To add the entry in the Windows registry on an AR agent system**
1. Select the HKEY_LOCAL_MACHINE\SOFTWARE\FirstSense\FirstSense key.
2. Create a new text string named "ApplicationPrograms".
3. Specify a value using the exact executable name including the .exe extension (case sensitive) in a comma-separated list such as “SAP.exe,OUTLOOK.exe”.

**Communication error...Unable to receive message...An established connection was aborted...**

**Symptom:**
If this series of error messages is persistent in a log file, you may have incompatible versions of Application Response components.

**Solution:**
Contact CA Technical Support for assistance.

**Default group “All-Clients” does not exist**

**Symptom:**
This error message appears if you renamed the default client set, All-Clients.

**Solution:**

**To resolve the error, undo the name change**
1. Stop the eHealth servers.
2. From the ehealth/data/response directory, make a backup copy of the Config.ard file and save it in a safe location.
3. Use a text editor to edit Config.ard as follows, where newAgentListName represents the name of the renamed All-Clients client set:
   a. In the TABLE unique_id, change the id of 'version' to a number that is at least 10 greater than the existing id number.
   b. In the TABLE machine_group, find the line that contains newAgentListName.
   c. Replace newAgentListName with All-Clients.
   d. Replace the description in the descr column with All Client Machines.
   e. Save the file.
4. Restart the eHealth servers.
   If your Application Response environment requires a custom name for the client set of all agents, create a client set with a custom name and then add all agents into it.

**Hook not loaded - IE, Exchange, or Windows**

**Symptom:**

Microsoft introduced a security setting called “Create global objects” in Windows 2000 SP4 and Windows 2003 Server that can interfere with the loading of hooks in a terminal services environment.

**Solution:**

All terminal services users must have privileges to create global objects or else the Windows hook and IE hook cannot load. For more information, refer to Microsoft Knowledge Base article 821546.

Do the following to help ensure that all terminal services users who log into systems with AR agents have privileges to create global objects:

**To assign privileges to users**

1. On the terminal server system, create a local group. Select Start, Programs, Computer Management.
2. Add users who will be monitored by Application Response to the new group.
3. Assign the Create global objects privilege to the new group:
   Start, Programs, Administrative Tools, Local Security Policy

The Hook not Loaded condition may also appear if Internet Explorer or Outlook is installed on the client system after the AR agent. In this case, register the appropriate hook with the application.
**Internet Explorer Hook not loaded**

**Symptom:**

IE does not find the IE hook, ariehook.dll file, and unregisters the dynamic link library (dll) file.

**Solution:**

Restore the dll file to the correct location and restart IE so it properly loads the file.

**To restore the dll file**

1. Close all instances of IE on the AR agent client system.
2. Change to the directory in which the AR agent is installed. 
   (C:\eHealth\agent\response is the default.)
3. Enter the following command to register the Application Response hook with IE:
   ```command
   regsvr32 ariehook.dll
   ```
4. Click OK.
5. Restart IE.

**JM: ServerName/AppName in RESPONSE_DATA message (unrecognized_info) doesn't EXIST...**

This error message indicates that Application Response corrects outdated information from the agent by using the AR controller’s configuration information. Ignore this message.

**Netscape Hook Not Loaded**

**Symptom:**

Netscape does not find the Netscape hook, arnetshk.dll file, and unregisters the dll file.

**Solution:**

Restore the dll file to the correct location and restart Netscape so it properly loads the file.

**To restore the dll file**

1. Close all instances of Netscape on the AR agent client system.
2. Change to the directory in which the AR agent is installed. 
   (C:\eHealth\agent\response is the default.)
3. Enter the following command to register the Application Response hook with Netscape:
   ```command
   regsvr32 arnetshk.dll
   ```
4. Click OK.
5. Restart Netscape.

**Outlook has problem loading the AR Exchange add-in during startup**

**Symptom:**

Outlook has an outdated file reference for the Exchange hook file.

**Solution:**

This may occur if you installed the AR agent in different locations on the same system: The AR agent installation program tries to prevent this.

To unregister and reregister the Exchange hook

1. Close all instances of Outlook on the client system.
2. Delete the following file that contains the working path to the location of the Exchange hook, where user represents the Outlook user name:
   
   C:\Documents and Settings\user\Local Settings\Application Data\Microsoft\Outlook\extend.dat

3. Change to the directory in which you last installed the AR agent.
   
   **Default:** C:\eHealth\agent\response

4. Enter the following command:
   
   `regsvr32 /u arexchhk.dll`

5. Click OK.

6. Enter the following command:
   
   `regsvr32 arexchhk.dll`

7. Click OK.

8. Restart Outlook.

**Source:** LoadFullList

**Message:** Connection failure

One or more of the following may apply to your situation.

**Symptom 1:**

The AR controller process (nhiArControl) is not running.

**Solution 1:**

Stop and restart the eHealth servers. If the process starts, check the AR Agent Management area of the eHealth Web user interface to confirm that the error is resolved.

**Symptom 2:**

The name of the default client set, All-Clients, may have been changed.
**Solution 2:**

On the Agent Set List page of the AR Agent Management area of the eHealth Web user interface, check that the name of the default client set, All-Clients, has not been changed. If it has been changed, undo the name change.

**To replace the default client set name**

1. Stop the eHealth servers.
2. From the ehealth/data/response directory, make a backup copy of the Config.ard file and save it in a safe location.
3. Use a text editor to edit Config.ard as follows, where newAgentListName represents the name of the renamed 'All-Clients' client set:
   a. In the TABLE unique_id, change the id of 'version' to a number that is at least 10 greater than the existing id number.
   b. In the TABLE machine_group, find the line that contains newAgentListName.
   c. Replace newAgentListName with All-Clients.
   d. Replace the description in the descr column with All-Clients.
   e. Save the file.
   f. Restart the eHealth servers.

   If your Application Response environment requires a custom name for the client set of all agents, create a client set with a custom name and then add all agents into it.

**Unable to connect to hostname in order to propagate messages...Could not resolve address...**

**Symptom:**

Indicate that a hostname is unresolvable using domain naming system (DNS).

**Solution:**

Ignore this issue because it does not impact Application Response functionality except for slightly reduced performance.

**Unable to execute CREATE UNIQUE INDEX**

**Symptom:**

If you run an At-a-Glance report on an Application Response path and the report fails with database errors, the problem may be caused by incompatible AR agents sending data to the eHealth database.

**Solution:**

Destroy the database using the nhDestroyDb command and then recreate it using the nhCreateDb command.
Common Symptoms

Unhandled exception in thread...

Symptom:
The associated agent is no longer able to monitor applications.

Solution:
Restart the agent. If the error occurs again, contact CA Technical Support.

Warning: (Controller0) Some AR Agents have active Conditions...

Symptom:
One or more AR agents are experiencing problems.

Solution:
Locate the Agent Condition Report at ehealth/data/response/agentcnd.log on the eHealth system. This report lists the hostname of the AR agent client system and the condition that is causing problems.

Common Symptoms

The following sections describe common symptoms and problems in alphabetical order, and possible solutions.

AR agents are listed but not running (red status)

When the AR controller has trouble communicating with the AR agent, confirm the following:
- The agents were published to monitor the correct applications
- The agents are configured with the correct hostname and port of the controller system
- The client systems rebooted after the AR agent installation
- The Application Response licenses are entered in eHealth
- On the AR agent systems, use the Services dialog to confirm that the AR agent process (Application Response Agent Proxy) is started.

AR agents are running (green status) but are not licensed (or will not stay licensed)

On the eHealth system, compare the number of agent licenses to the number of active agents listed in the ehealth/data/response/arlicense.csv file.
If the number of active, running agents exceeds the number of AR agent licenses, you must either purchase more agent licenses, uninstall some agents, or turn some agents off.

**Note:** For more information about agents licenses and turning off agents, see the eHealth Help, Application Response. For information about uninstalling agents, see Uninstall AR Agents.

### AR agents do not appear in the Agent List

One or more of the following conditions may apply:

- If no AR agents appear in the Agent List page, wait a few minutes and then click Refresh Data. It can take up to 15 minutes for AR agents to register with the eHealth (AR controller) system.

- Your Web browser must be set to update with every visit to a web page. If you use Internet Explorer, you can check for this by doing the following:
  1. Select Tools, Internet Options.
  2. In the Internet Options dialog, select the General tab; then click Settings under Temporary Internet files.
  3. In the Settings dialog, select Every visit to the page; then click OK.
  4. Click OK to close the Internet Options dialog.
  5. On the Agent List page of the AR Agent Management area of the eHealth web user interface, click Refresh Data. The page should display an updated list of agents.

- Firewall or anti-virus software packages may be preventing the exchange of Application Response files. Problems have been reported with Norton SystemWorks anti-virus software, Tiny Personal Firewall version, and McAfee Firewall. Contact CA Technical Support for possible workarounds.

- Network Address Translation may prevent the exchange of Application Response files. Contact your IT staff to determine if this issue exists in your environment.

- An Access Control List may prevent the exchange of Application Response files. Contact your IT staff to determine if this issue exists in your environment.

- On each of the AR agent systems that are not registering, open a command prompt window and enter the following command to confirm that each system can communicate with the eHealth system and resolve the hostname of the eHealth system:

  `ping hostname of eHealth system`

- If a bad address error appears, publish a new agent installation program that uses the Internet Protocol (IP) address of the eHealth system (instead of the hostname), and redeploy the AR agents.

- Check the following registry key to confirm that it contains the hostname of the correct AR controller:

  `HKEY_LOCAL_MACHINE\SOFTWARE\FirstSense\FirstSense\ControllerHost`
If the hostname in the registry does not match the hostname of the eHealth system, publish a new agent installation program that uses the correct hostname of the eHealth (AR controller) system and redeploy the AR agents.

AR agent does not start

If this problem occurs following a new installation, check the following:

- Confirm that agents are installed on systems with one of the following operating system platforms:
  - Windows XP
  - Windows 2000 Professional
  - Windows 2000 Server
  - Windows NT Workstation 4.0, SP 3+
  - Windows NT Server 4.0, SP 3+
  - Windows 98 Second Edition
  - Windows 98
  - Windows 95

- If you are running eHealth Release 5.6.5 or later, confirm that the agents do not use TCP/IP over a non-supported network medium such as Token Ring.

- Firewall or anti-virus software packages may be preventing the exchange of Application Response files. Problems have been reported with Norton SystemWorks 2003 anti-virus software, Tiny Personal Firewall version 2.0.2.85, and McAfee Firewall. Contact CA Technical Support for possible workarounds.

If this problem occurs following a manual agent upgrade, it is likely that the AR agent did not uninstall completely and/or that the AR agent installation package was bad. Do the following:

1. Uninstall the AR agent.
2. To confirm that the removal is complete, make sure that the FirstSense Agent branch is no longer in the Windows registry as follows:
   a. In a command prompt window, open the Registry Editor window by entering: regedit
   b. Navigate to HKEY_LOCAL_MACHINE\Software\FirstSense.
   c. Confirm that FirstSense is not in the hierarchy.
   d. Reinstall the AR agent using a known good package.

AR agent is slow to restart following the ARWatch Not Running condition

One or more of the following conditions may apply:

- If an AR agent has the ARWatch Not Running condition and AR is running in a traditional, single-client/server environment (not a terminal services environment), restart the ARAgent Proxy service on that system.
To restart the ARAgent Proxy service

1. On the Windows desktop, right-click on the system icon.
2. Select Manage.
3. In the Computer Management dialog, select Services and Applications.
4. Select Services.
5. In the list of services, select Application Response Agent Proxy.
6. Click Start.

If the process stops again, contact CA Technical Support.

- If an AR agent has the ARWatch Not Running condition and AR is running in a terminal services environment, the ARWatch process may have ended prematurely because of a missing a registry entry, or the entry may be missing the name of the application.

To add the entry in the Windows registry on an AR agent system

1. Select the HKEY_LOCAL_MACHINE\SOFTWARE\FirstSense\FirstSense key.
2. Create a new text string named "ApplicationPrograms".
3. Specify a value using the exact executable name including the .exe extension (case sensitive) in a comma-separated list such as "SAP.exe,OUTLOOK.exe".

Data in AR reports appears to be inaccurate

One or more of the following conditions may apply:

- If eHealth is receiving data from the registered clients, do the following:
  1. Verify that you ran the report on the correct path element and that you understand the descriptions of the selected variables. For descriptions of report variables, see the eHealth Help.
  2. Compare the values returned by Application Response with your own measurements using a stopwatch.
  3. If evidence indicates that the Application Response data is incorrect, forward the following information to the CA Technical Support site for further assistance:
     - The report (ASCII format) that seems to include incorrect data
     - The data from the external source that conflicts with the report data
     - The event log file: ar_agent/agent/response/Events.btl (where ar_agent is the full path to the directory in which you installed the AR agent)
     - The transaction log file: ar_agent/agent/response/BTUsage.csv
     - If applicable, the custom rule used to gather the data (ehealth/data/response/rules.ard file, where ehealth is the full path to the directory in which you installed eHealth)
If you run Application Response reports from a Distributed eHealth Console, they may contain incomplete information and charts might be missing because the Distributed eHealth System does not replicate new Application Response application types to Distributed eHealth Consoles. (It does, however, replicate the groups that contain these elements.) Always run the reports from the Distributed eHealth System on which Application Response is installed.

Data in AR reports appears to be inconsistent

If a report shows inconsistent data for some agents, those agents may have had intermittent problems communicating with the AR controller system; agents temporarily save transaction information to the arusage file called which resides in the agent's home directory (C:\eHealth\agent\response by default). If possible, confirm that all agents have sent any saved data to the AR controller system. On each system, confirm that the file size of the arusage file is zero. Run reports for those AR agents only.

Data in AR reports appears to be skewed

All data in a group Trend report for Application Response data must have the same sample size. Do not run group Trend reports that cross data-rollup boundaries and use the most granular sample size. For example, if data rollups occur every three days, do not run a group Trend report for the last 7 days. If you do, a significant shift in the data will occur at the three-day rollup boundary.

No Application Response data

One or more of the following conditions may apply:

- Application Response either cannot support or requires customized rule sets to monitor the following application types:
  - Java applications
  - TN3270 applications
  - Web based applications that utilize frames
  - Applications that require monitoring events in child windows
  - Applications with owner-draw controls
- On the Application List page of the AR Agent Management area of the eHealth Web user interface, confirm that the application has been enabled for monitoring.
- If the application was started on the client system before the AR agent started, the agent does not recognize transactions. The end user must start a new instance of the application for transactions to be recognized.
- If application hooks are loaded and communication between the AR agent and controller are confirmed, default rules may not be matching any transactions. If you have BT Studio, you can compare event definitions in default rules to an actual event log.
To compare default rule definitions and event logs

1. On the Agent Properties page of the AR Agent Management area of the eHealth Web user interface, turn on event recording for the AR agent system.
2. Perform application transactions, which are recorded in the events.btl file.
3. Open the events.btl file in BT Studio and filter the events based on the executable name of the application.
4. Run the events.btl file against the default rule set.
5. In the Results Pane, compare the recognized transactions to the event definition in the default rules.
6. Modify the default rules so that they match the events that you want.

Example: Modified Rule Set for Monitoring IE Transactions

```plaintext
transaction "query"
    module "ar2"{
        # Differentiate specific mouse click by adding the Class statement
        event "query1" Windows MouseClick {Class="Internet Explorer_Server"}
        # Look at frame rather than top level of Web page and match URL
        event "query2" Web BeginLoad {Level="sublink" URL=contains:"<unique fragment>"}
        # Look at frame rather than top level of Web page and match title
        event "query3" Web EndLoad {level="sublink" Title=contains:"<Customer Title>"}
    }
```

If the lack of data is specific to Citrix published applications, the applications may be missing a registry entry, or the entry may be missing the name of the application.

To add the entry in the Windows registry on an AR agent system

1. Select the HKEY_LOCAL_MACHINE\SOFTWARE\FirstSense\FirstSense key.
2. Create a new text string named "ApplicationPrograms".
3. Specify a value using the exact executable name including the .exe extension (case sensitive) in a comma-separated list such as "SAP.exe,OUTLOOK.exe".

To add the registry entry using the eHealth Web user interface

1. On the Agent List page of the eHealth Web user interface, click the name of an agent system.
2. On the Agent Properties page, click Configure Agent.
3. In the Name field or the New Custom Setting area, enter the following: ApplicationPrograms
4. In the Type field, select String.
5. In the Value field, enter the names of the executables (without the .exe file type extension) separated by commas. For example to monitor Microsoft IE and Outlook, you might enter the following: IEXPLORE, OUTLOOK

6. Click Insert.

7. In the Insert the following Custom Value? dialog, check the accuracy of the information.

8. If the information is correct, click OK.

9. Click Apply.

eHealth defines the registry setting on the AR agent system within 30 seconds.

- The lack of Application Response data may be caused by a significant difference between system times of the Application Response client and the eHealth server. eHealth stores Application Response data using the client system time, while eHealth reports are based on the system clock of the eHealth system. Synchronize the clock on the client system with the clock on the eHealth system. You can use time synchronization software such as Network Time Protocol (NTP).

**No data in response path reports, and/or response paths not created in Path/PVC Manager**

Confirm that Application Response for your agent is configured correctly and verify the response paths are correct by following this process:

1. On the Agent List page of the AR Agent Management area of the eHealth Web user interface, confirm that the AR agent is running and licensed.

2. If the agent is not running, click the agent name to display the Agent Properties window and check the Conditions field for error conditions.

3. On the Application List page of the AR Agent Management area of the eHealth Web user interface, confirm that the application has been enabled for monitoring.

4. Confirm that end users are using the application to perform transactions on the client system. It can take up to 15 minutes for the AR agent to record a transaction and have it appear in eHealth.

5. Confirm that the non-default server definition exists by doing the following:
   a. On the Server List page of the AR Agent Management area of the eHealth Web user interface, select the name of the server in the response path.
   b. On the Server Properties page, confirm that the hostname, port number, and server type are correct.
   c. If necessary, make modifications and click OK.

6. Confirm that the server definition is associated with the correct application by doing the following:
   a. On the Application List page of the AR Agent Management area of the eHealth Web user interface, select the name of the application that should be associated with the non-default server.
b. On the Application Properties page, confirm that the non-default server appears in the list and that a checkmark appears in the Attached column.

7. Confirm that client systems with AR agents are communicating with the destination server.

8. Confirm that the AR agent is recording transactions by enabling transaction logging, and verifying the transactions by using the Agent Transaction Viewer (ATV). If transactions exist in the ATV, data should appear in the report.

9. If transactions appear in the ATV, use the Path/PVC Manager to determine the path to which this data will be associated by noting the client system name, the application, the module, and the destination server. The name of the path appears in the Path/PVC Manager according to the following syntax:

   `<Client name> - <app> - <module> - <destination server>`

   eHealth only creates a response path after application activity occurs. If an end user performs application activity at 6:00, the corresponding response path may not appear in the eHealth console for another 30 minutes, at 6:30.

   **Note:** When you run a report, make sure that you select the correct response path.

**No Windows events**

If process and connection events appear in BT Studio but Windows events do not, try stopping and restarting the agent and restart the monitored applications.

**Response data in reports is sparse**

One or more of the following conditions may apply:

- Application Response collects data based on user activity. If user activity is intermittent and a small number of users are being monitored, the resulting data will be sparse. To prevent sparse data, do any of the following:
  - Monitor more users
  - Use WinTask and Service Availability to play back scripts that mimic user activity
- Using the Data Rollup scheduled job, eHealth aggregates data to prevent the database from growing rapidly. As-polled data that appeared to be continuous may have wider gaps after the data rollup. You can increase the granularity of eHealth data in reports by increasing the number of days of as-polled data saved in the database. However, you should make sure that your database has additional capacity for rapid growth.
Response paths for Application Response do not appear

If response paths for Application Response do not appear in the eHealth console, do the following:

- Confirm that the agent has a license.
- Make sure that users have been performing tasks using the monitored applications. Also, note that it can take 30 minutes from the time that a user performs a task until eHealth creates a corresponding response path.

Response (AR Path) Report fails

If database errors appear when an AR path At-a-Glance report fails, investigate whether incompatible AR agents could be sending data to the eHealth database. To resolve the problem, you may have to destroy the database using the `nhDestroyDb` command and then recreate it using the `nhCreateDb` command.

Information to Collect for CA Technical Support

If you determine that you need to contact CA Technical Support, do the following:

1. Turn on transaction logging for a specific agent on the Agent List page in the AR Agent Management area of the eHealth Web user interface.
2. Turn on event logging for a specific agent on the Agent Properties page in the AR Agent Management area of the eHealth Web user interface.
3. Reproduce the problem.
4. Stop the AR agent.
5. Send e-mail describing the problem and attach the following files from the AR agent system (`ar_agent\agent\response`, where `ar_agent` is the full path to the directory in which you installed the AR agent) to support.concord.com
   - `aragent.database`
   - `arproxy.log`
   - `aragent.log`
   - `BTUsage.csv`
   - `BTUsage.csv.old`
   - `Events.btl`
   - `Events.btl.old`
   - `agent.debug.log`
   - `agent.debug.log.old`

You can obtain all of these files by opening the Agent Properties window in the AR Agent Management area of the eHealth Web user interface and selecting Export Agent Files.
6. Send email describing the problem and attach the files in the ehealth/data/response directory, where ehealth is the full path to the directory in which you installed eHealth, to support.concord.com.
Index

A
Agents
AR • 8
Cisco IP SLA • 9
Juniper RPM • 10
SystemEDGE • 9
Application Response
overview • 8
performance considerations • 18
applications
default • 14
AR agent
licensing • 17
measuring transactions • 16
monitoring • 16
AR Agent Publisher
default installation program • 19
AR Controller, agent registration • 21
At-a-Glance reports • 51
C
Cisco
jitter protocols • 30
ping protocols • 31
Cisco IP SLA
creating response destination elements • 28
creating response paths • 30
overview • 9
Cisco SA Agent, overview • 9
Creating
destination elements • 28
response paths • 30
D
Deleting, response elements • 40
Destination elements
creating • 28
modifying • 39
Destinations, Health report • 53
Dialog box
Add Destination Element • 28
Modify Path Element • 37
Modify Path Elements • 38
Response Path Manager • 35
Discover
overview • 27
scheduling • 28
Disman
ping protocols • 31
pre-existing response paths • 27
E
eHealth
collecting data from AR agents • 16
reports, average application response time • 16
eHealth Response
element naming conventions • 32
elements
discovering • 27
enabling data collection for AR agents • 17
managing for reports • 43
nhGetRespLimit utility • 48
overview • 7
polling errors • 33
protocols • 30
reports, running • 50
response path elements, creating • 31
response paths, creating • 30
Elements
deleting • 40
destination • 28, 39
naming conventions • 32
source • 39
G
Group lists
creating for response • 47
response • 46
Groups
creating for reports • 46
response • 46
used as filter for console and Web • 46

Health reports • 53
for response • 53
response, Elements • 53

Installing AR agents
about • 18
IP SLA
creating response destination elements • 28
creating response paths • 30
overview • 9

Jitter
Cisco measurement • 9
Cisco protocols • 30
Juniper definition • 10
Juniper protocols • 30
Juniper RPM
creating response destination elements • 28
creating response paths • 30
jitter definition • 10
jitter protocols • 30
overview • 10
ping protocols • 31

Licensing, AR agent • 17
Live Exceptions, monitoring elements • 36

Modifying
destination elements • 39
response paths • 37
source elements • 39

Naming conventions, response elements • 32
Network resources • 10
nhSetRespLimit utility • 48

Packet loss • 9
Path builder • 32
Path Summary reports • 44

Paths
AR • 33
deleting • 41
Health report • 53
modifying • 37
pre-existing • 27
response • 11, 30
paths.cfg.log file • 36
Ping protocols
Cisco • 31
Disman • 31
Juniper • 31

Recommendation file, specifying • 50
Reports
At-a-Glance • 51
CIO SLR • 44
Cisco IP SLA reports • 9
Health • 53
health • 53
Juniper RPM reports • 10
Path Summary • 44
response • 43
response sources, destinations, and paths • 43
response summary • 54
running • 50
Service Level, response • 53
trend • 52
Trend reports • 52
Response
adding paths • 31
deleting paths • 41
element naming conventions • 32
endpoints • 53
Health report • 53
modifying paths • 37
reports • 43
saving paths in file • 36
summary report • 54
Response destination
adding elements to the poller configuration • 28
creating • 28
elements • 28
troubleshooting • 33
response destination
about • 11
Response elements
deleting • 40
managing • 35
naming • 32
Response limit
definition • 47
evaluating • 48
recommending and setting • 47
response path
about • 11
Response paths
adding elements to the poller configuration • 31
AR • 33
creating • 11, 30
deleting elements • 40
managing • 35
managing elements • 35
modifying • 37
polling errors • 33
pre-existing • 27
Response report types • 44
response source
about • 11
Response source, modifying elements • 39
Response summary reports • 54
Response time, monitoring with eHealth • 11
RFC2925
pre-existing response paths • 27
RPM
creating response destination elements • 28
creating response paths • 30
overview • 10
RTTMON, Cisco • 30
Running reports • 50
S
Scheduling discover • 28
servers
default • 14
Service Availability • 9
Service Level reports, response • 53
Source elements, modifying • 39
SystemEDGE, plug-in modules • 9
T
terminal servers
licensing AR agent for • 17
Trend reports • 52
U
uninstall program, for AR agents • 26
V
Variables
NH_RTR_ZERO_DATA_POLLS • 33
Voice Quality Monitor • 9
VQM
overview • 9