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
- eHealth Network Management .................................................. 11
- Types of eHealth Systems ........................................................... 11
  - Standalone eHealth System ....................................................... 12
  - Distributed eHealth System ...................................................... 12
  - Remote Polling System ............................................................ 12
  - Traffic Accountant System ....................................................... 13
- How to Administer an eHealth System ........................................ 13
- Administrator Roles ................................................................. 13
- eHealth Software Maintenance .................................................. 14
- eHealth User Interfaces ............................................................ 14

### Chapter 2: Configuring the eHealth Administration User Interfaces
- The eHealth Console ............................................................... 17
  - How to Access the eHealth Console on a Windows System .......... 17
  - Display Alias Names ............................................................. 19
  - Enable Time Zone Setting in Report User Interface .................. 20
  - Set Date and Time Formats .................................................... 20
- The OneClick for eHealth Console ............................................. 21
  - Access the OneClickEH Console .............................................. 21
  - Set Up the OneClick for eHealth Console ................................ 22
- eHealth Command Line Interface .............................................. 25
  - How to Use the Command Line Interface .................................. 25
- The eHealth Web User Interface ................................................. 26
  - Log In to the eHealth Web User Interface ................................. 26
- eHealth Product Licenses .......................................................... 28
  - Track License Status and Usage ............................................. 28
  - How to Add eHealth Licenses .................................................. 29
- SSL Protocol ........................................................................... 31
  - SSL in the eHealth Environment ............................................. 31
  - Generate a Private Key and Certificate Signing Request ............ 32
  - Enable SSL ................................................................. 33
  - Disable SSL ............................................................... 34
  - Add a Self-Signed Certificate to the Live Health Client ............ 35

### Chapter 3: Discovering Resources
- eHealth Discovery ................................................................. 37
  - Discover Methods .............................................................. 37
  - How eHealth Discovers Resources ........................................... 38
  - How to Identify Your Infrastructure Resources .......................... 38
  - How to Discover Resources Interactively ................................ 39
  - How eHealth Creates a Modem Pool Element ............................ 42
Discover Log File ................................................................. 43
Discover Log Contents .......................................................... 44
How to Resolve a Missing Element ............................................. 46
How to Resolve a Duplicate Key .................................................. 46
How to Resolve a Duplicate Element Name ................................... 46
How to Address Unresolved Updates .......................................... 47
Rediscovery .............................................................................. 47
How to Tailor Your Discovery ..................................................... 48
How to Configure eHealth to Discover SNMPv3 Elements ............... 52
How to Increase the Number of Devices That eHealth Discovers ...... 53
How to Automatically Save to Groups during a Discovery ................ 53
Community Strings ................................................................. 53
Enable eHealth to Find System Processes ..................................... 54
Maintain Data Continuity for Rebooted Systems ............................. 56
Scheduled Discover Job ........................................................... 57
How eHealth Saves the Results of a Scheduled Discover Job ............ 57
How to Run Effective Scheduled Discoveries ................................. 57
Set Up a Scheduled Discover Job ............................................... 58
How to Improve Your Discoveries .............................................. 59

Chapter 4: Maintaining Your Element Configuration

Elements .................................................................................. 61
View Your Element Configuration .............................................. 61
How to Save Element Information .............................................. 63
The eHealth Poller ...................................................................... 64
How to Maintain the eHealth Element Configuration ....................... 67
Poller License Consumption ....................................................... 68
How to Manage Poller License Consumption ................................. 68
Common Polling Problems ......................................................... 69
How to Resolve Common Polling Problems ................................... 69
Element Properties ..................................................................... 76
How to Update the Properties of an Element .................................. 78
How to Use DCI to Modify Element Information .............................. 83
Element Removal ....................................................................... 83
How to Delete Elements .......................................................... 84
How to Retire Elements .......................................................... 85
Element Creation ....................................................................... 85

Chapter 5: Organizing Your Element Configuration by Grouping

The Grouping Capability .......................................................... 89
How to Use OneClickEH to Create a Group of Elements .................. 90
Group and Group List Creation .................................................. 90
Group Management ................................................................... 94
Chapter 6: Configuring eHealth User Account Permissions

Web User Account Permissions .......................................................... 101
Create a Web User Account .............................................................. 101
How to Change Web User Account Permissions ............................... 103
Set OneClickEH Admin Permissions ............................................... 104

Chapter 7: Database Management

The eHealth Database ........................................................................ 109
The Role of the eHealth Database Manager ...................................... 110
eHealth Database Sizing ................................................................. 111
How to Monitor Disk Space Allocated for Backups .......................... 112
Check Disk Space ........................................................................... 113
Scan Log Files for Errors ............................................................... 114
Factors that Drive Database Growth ................................................ 114
Statistics Rollup Scheduled Job ....................................................... 117
Live Exceptions Baseline Scheduled Job .......................................... 119
Live Exceptions History Scheduled Job .......................................... 119
Delete Database Archive Logs Scheduled Job ................................ 119
Database Maintenance Scheduled Job ............................................ 120
Delete Temporary Tables Scheduled Job ........................................ 120
Delete Old Reports Scheduled Job ................................................ 120
Conversations Rollup Scheduled Job ............................................... 121
Cleanup Nodes Scheduled Job ....................................................... 121
FSA Scrubber Scheduled Job .......................................................... 122
eHealth Database Backups .............................................................. 122
Incremental Saves .......................................................................... 123
Universal (ASCII) Saves ............................................................... 124
How Database Saves Work ........................................................... 124
Perform a Full Database Save ....................................................... 126
Best Practices for Database Backups .............................................. 127
Modify a Incremental Save Scheduled Job ..................................... 129
Schedule Full Database Saves ....................................................... 130
Monitor Disk Space Available for Backups ..................................... 131
How to Recover the Database from a Backup ............................... 132
Perform Point-in-Time Recovery from an Incremental Backup ........ 134
Move Distributed eHealth Databases ............................................. 139
Stop the Database ......................................................................... 139
Establish Database Security .......................................................... 140
Change User Passwords ............................................................... 140
Resize the eHealth Database ......................................................... 143
View the Status of the Database .................................................... 145
Examine the Disks ......................................................................... 148
How to Reclaim Disk Space .......................................................... 149
Add a Datafile ............................................................................... 151
Move a Datafile ............................................................................. 151
Chapter 8: Monitoring eHealth System Processes and Activities

eHealth’s Self-Monitoring Capabilities .................................................. 153
Track OneClickEH Administration Changes ........................................ 154
Track Element Changes in the Database ................................................. 155
Track System Events .............................................................................. 155
Monitor Scheduled Job History ............................................................... 156
Monitor Web Activity ............................................................................. 157
Monitor Database Alerts ......................................................................... 158
Manage eHealth System Files ................................................................. 158
Monitor eHealth System Processes ......................................................... 159

Chapter 9: Managing Scheduled Jobs

eHealth Scheduled Job ........................................................................... 161
The eHealth Job Scheduler ..................................................................... 161
How to Monitor Scheduled Jobs and Identify Problems ......................... 162

Chapter 10: Managing and Monitoring Systems

System Data Collection ........................................................................... 171
How to Configure eHealth to Collect Data from Unicenter NSM System Agents .................................................. 171
How the SystemEDGE Agent Collects Data ........................................... 172
SystemEDGE Self-Monitoring Features ................................................ 172
How You Can View System Data and Manage SystemEDGE Agents .... 173
Discover System Elements ................................................................... 173
Collect Data from System Elements ...................................................... 174
Schedule Configuration Update for System Elements ......................... 174
View Unlicensed SystemEDGE Agents ................................................ 175
System Process Set Configuration .......................................................... 175
Process Set Usage ................................................................................. 176
Use Discover Rules to Discover Process Sets ....................................... 176
Report on Individual Process Elements in a Process Set ....................... 177
Create a Process Set for an Application ................................................ 177
Delete Processes from a Process Set Definition .................................... 179
Delete a Process Set Definition ............................................................. 179
Example: Create a Process Set .............................................................. 179
Sample Reports for Process Sets ........................................................... 181
How to Resolve System Polling Errors .................................................. 182
Resolve Excessive Use of Disk Space by SystemEDGE Log Files .......... 182
eHealth Reports for Systems ................................................................. 182
At-a-Glance Reports for Systems ......................................................... 184
Trend Reports for Systems ................................................................. 184
Top N Reports for Systems ................................................................. 184
What-If Capacity Trend Reports for Systems ....................................... 184
MyHealth Reports for Systems ............................................................ 185
Health Reports for Systems ................................................................. 185
Service Level Reports for Systems ....................................................... 185
Using Live Health with the SystemEDGE Agent ................................... 186
Chapter 11: Managing and Monitoring Applications

Guidelines for Monitoring Applications .......................................................... 187
Application Data Collection ............................................................................ 188
Discover Application Elements ..................................................................... 190
Schedule Data Collection for Application Elements .................................... 191
Delete an Application Element ..................................................................... 192
Create Application Groups .......................................................................... 192
Create Application Group Lists ................................................................... 192
Run eHealth Reports for Applications ............................................................ 193
At-a-Glance Reports for Applications ............................................................... 194
Trend Reports for Applications .................................................................... 194
Top N Reports for Applications .................................................................... 195
MyHealth Reports for Applications ................................................................. 195

Appendix A: The Discover Algorithm

eHealth Discover Matching Algorithm ............................................................ 197
How eHealth Matches at the Device Level ..................................................... 198
How eHealth Matches at the Agent Level ....................................................... 198
How eHealth Matches at the Element Level .................................................. 199
How eHealth Matches Discover Keys ............................................................ 199
How eHealth Matches at the Physical Address Level .................................... 202
How eHealth Matches MIB Attributes ........................................................... 202

Appendix B: eHealth Element Naming Conventions

LAN/WAN Element Discovery ...................................................................... 205
Router/Switch Element Discovery .................................................................. 206
Traffic Accountant Element Discovery ........................................................... 207
System Element Discovery ............................................................................ 208
Application Element Discovery ..................................................................... 208
Modem Pool and RAS Element Discovery .................................................... 209
Response Element Discovery ....................................................................... 210
QoS Element Discovery .................................................................................. 210
How eHealth Names Elements ..................................................................... 211
How to Customize Element Names ............................................................... 214

Appendix C: Managing Alternate Latency

Latency ........................................................................................................... 217
Alternate Latency Collection ......................................................................... 217
How to Configure the Alternate Latency Ping Process .................................. 218
Alternate Latency Guidelines ......................................................................... 219

Appendix D: Using Secondary Consoles

Administration with Multiple Consoles .......................................................... 221
Configure Secondary Consoles on UNIX Systems ....................................... 224
Configure Secondary Consoles on Windows Systems .................................. 225
Appendix E: Customizing the eHealth Web User Interface and OneClickEH

Customize the eHealth Web Site .................................................. 229
  How to Customize a Privacy Page for Your eHealth Site ...................... 232
  How to Customize the Gateway Page for a Web User Account ................. 232
  How to Customize the Gateway Page for the eHealth Site .................... 232
  How to Customize the eHealth Help ......................................... 233
  Customize Logo Images and Link Destinations ................................ 233
  How to Create Report Shortcuts ............................................ 234
  Provide Report Shortcuts for an eHealth Site or Individual Users ............ 235
Advanced Customization of the Web User Interface ............................. 237
  Creating Customized Links .................................................. 237
  Creating Links to eHealth Applications ..................................... 238
  Link to an Expanded Organization Page .................................... 241
  Create Links to Generate Reports Automatically ............................. 258
  How to Customize the Apache Web Server ................................... 259
  Displaying Alias Names in eHealth ......................................... 262
  Set the Date Format in eHealth ............................................. 263
  Set the Time Format in eHealth ............................................. 264
  Specify Date and Time Preferences for the OneClick for eHealth Interface ...... 265
  Customize the User Administration Screen of the OneClick for eHealth Interface . 266
  Customize OneClickEH Tables ............................................... 266
  Save OneClickEH Table Entries ............................................. 267

Appendix F: Troubleshooting and Best Practices for Administering eHealth

Create Technical Support Information ....................................... 269
  Enable Advanced Logging for Web Server Processes ....................... 270
  Enable Advanced Logging for eHealth System Processes .................... 271
  Devices Lose Data before eHealth Can Collect It ........................... 272
  Discover Log Reports Several Suspected Duplicates ......................... 273
  eHealth Web Server Is Inaccessible on a Windows System ................... 273
  eHealth Web Server Is Inaccessible on a UNIX System ...................... 274
  eHealth Generates Error after Changing Date or System Time ................ 275
  OneClickEH Installation Fails ............................................... 275
  Statistics Polling Errors Remain after Being Resolved ....................... 276
  Poll Durations Are at or near the Normal Polling Interval .................. 276
  Some Elements Are Not Selectable in the Element Tables .................... 277
  Able to Log In to OneClickEH without Supplying a Password ................ 277
  Disable the Automatic Login for an eHealth System ........................ 278
  Fail to Discover a PVC for an ATM Probe .................................. 279
  Fail to Discover Multiple Routers with Channels ............................ 279
  Unable to Identify SNMP Agents That Allow eHealth to Discover Systems ..... 280
  Unable to Determine Which Systems to Poll .................................. 280
  Encounter a Fatal Error on a UNIX System after a Discover .................. 281
  Unable to Discover Gigabit Ethernet Interfaces on a System ................. 282
  Unable to Perform a Discovery for a Particular Technology ................ 283
  Unable to Save Data for an Element in the Database ........................ 283
  Receive Incorrect Line Speeds on Devices after Discovery .................... 284
  Reporting No Data for New Variables ....................................... 284
Chapter 1: Overview

This chapter contains the following sections:

- eHealth Network Management
- Types of eHealth Systems
- Administrator Roles
- eHealth Software Maintenance
- eHealth User Interfaces

eHealth Network Management

Through the process of discovery, eHealth locates the resources within your infrastructure. Using Simple Network Management Protocol (SNMP) agents, it searches for the IP addresses that you specify (in v4 or v6 format), obtains information from the management information base (MIB) of each agent, and creates elements based on that information. After it stores the element information in its database, the eHealth poller automatically collects data for the elements.

Types of eHealth Systems

eHealth offers several different types of systems for managing the performance of the resources within an infrastructure:

- Standalone
- Distributed
- Remote Poller
- Traffic Accountant

The type of system that you choose depends on the size of the infrastructure, the number of resources within the network, and the types of resources that you want to monitor.
Types of eHealth Systems

Standalone eHealth System

A standalone eHealth system is a single workstation on which you have installed the eHealth software. Standalone eHealth systems typically support up to 50,000 elements. Depending on the size of your infrastructure, you may only need to install a single eHealth system to manage your resources. If your organization is extensive, but you do not need to report on all elements together in one report, you can install multiple standalone eHealth systems throughout your organization, each administered by a different person. Standalone systems are not connected in any way, and each one must collect and process the data for the resources that it monitors.

Distributed eHealth System

If you have a large infrastructure, you could deploy multiple Distributed eHealth Systems across large geographic ranges or locate them centrally to gather data and manage various segments of your network. This configuration is referred to as a cluster.

The cluster contains several eHealth systems that manage specific sets of resources and share the information with each other. By using Distributed eHealth, you can distribute the workload of collecting and processing data across multiple eHealth systems that work in parallel. Report users can access reports for any elements or groups in the cluster from Distributed eHealth Consoles, which are reporting front-ends to the cluster. Clusters can support up to one million elements. For complete instructions on administering a cluster, see the Distributed eHealth Administration Guide.

Remote Polling System

If you are administering a large-scale or wide-area environment, one eHealth system may not be enough to monitor all of your resources. As an alternative to a Distributed system, you can use a remote polling environment. With remote polling, you install eHealth on remote systems (called remote sites) and configure each site to poll a set of elements. The database at each remote eHealth site contains the data for the elements that it is polling, and you can use eHealth at each site to manage those elements. A central eHealth system retrieves element information and performance data periodically from the remote eHealth systems, and then merges the data into one central eHealth database.

From this central database, you can run reports for all elements. The central site can support up to 50,000 elements, depending on the system configuration and the reports that you run. For complete instructions on administering a remote poller system, see the eHealth Remote Poller User Guide.
Traffic Accountant System

Traffic Accountant is a specialized network and application monitoring capability. Rather than collect data on statistics from network resources such as routers/switches, interfaces, and systems, it collects traffic flow information from RMON2 probes and traffic sources such as Cisco NetFlow devices. It provides network traffic analysis and reporting that enables you to track the individual users, applications, and departments who are consuming most of your network resources.

Because the volume of Traffic Accountant data can become quite large and consumes a large amount of data storage capacity, you must install the application on a separate system that is dedicated to eHealth Traffic Accountant. CA does not support the installation of eHealth statistics monitoring and Traffic Accountant on a single system. For instructions on administering a Traffic Accountant system, see the eHealth Traffic Accountant and Cisco NetFlow Administration Guide.

How to Administer an eHealth System

eHealth administration involves using the standard eHealth software product to report on the performance of the resources within your network that support your business and operations.

To administer an eHealth system, do the following:
1. Use eHealth to discover your resources, and then poll them to collect data on their performance.
2. Organize your elements by grouping them based on function or location.
3. Maintain the eHealth element configuration to enable eHealth to continue to collect data on the resources.
4. Monitor system processes, logs, scheduled jobs, and database space so that eHealth can function properly.

Administrator Roles

For most eHealth sites, the eHealth administrator who manages the eHealth console is also the administrator of the eHealth Web user interface and OneClick for eHealth console. However, in larger sites, these responsibilities are shared by several people.

- To administer the eHealth console and CLI, you must log in to the eHealth system using an operating system account that has eHealth administration privileges.
- To administer OneClickEH and the eHealth Web user interface, you must log in to the eHealth system using a special eHealth web user account named admin. This account allows you to configure these interfaces, control access to them, and assign limited administrative privileges to other users. By default, the eHealth web user account cannot log in to OneClickEH.
When a new release of eHealth is available, you should upgrade to obtain the latest features and software fixes. The InstallPlus program allows you to reduce downtime by installing the very latest fixes, certifications, and support as part of your upgrade. The InstallPlus program is the standard eHealth installation program—it is updated for every patch and certification release. The program provides the very latest available software when you install or upgrade to an eHealth release.

Use the InstallPlus program only when you install an eHealth release for the first time, or when you first upgrade from a previous eHealth release. For instructions on using InstallPlus, see the *eHealth Installation Guide*.

**eHealth User Interfaces**

The standard eHealth product is composed of an integrated database and four user interfaces. Not all functions are available through every eHealth interface, and some are available in more than one.

<table>
<thead>
<tr>
<th>User Interface</th>
<th>Primary Administrative Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth console</td>
<td>■ Manage response path elements.</td>
</tr>
<tr>
<td></td>
<td>■ Manage alternate latency.</td>
</tr>
<tr>
<td></td>
<td>■ Create and modify scheduled report jobs.</td>
</tr>
<tr>
<td></td>
<td>■ Change global console settings.</td>
</tr>
<tr>
<td></td>
<td>■ Run and customize standard reports.</td>
</tr>
<tr>
<td></td>
<td>■ Manage service profiles and update element information.</td>
</tr>
<tr>
<td></td>
<td>■ Load a new database, and save (back up) your database.</td>
</tr>
<tr>
<td></td>
<td>■ Save system messages to a log file.</td>
</tr>
<tr>
<td></td>
<td>■ Import NetFlow data and configure the eHealth Import Poller.</td>
</tr>
<tr>
<td>eHealth Web user</td>
<td>■ Design a gateway page as a portal to your site.</td>
</tr>
<tr>
<td>interface</td>
<td>■ Design customized report pages for individual users.</td>
</tr>
<tr>
<td></td>
<td>■ Customize the eHealth Web site.</td>
</tr>
<tr>
<td></td>
<td>■ Access the Report Center to create customized reports.</td>
</tr>
<tr>
<td><strong>User Interface</strong></td>
<td><strong>Primary Administrative Functions</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>eHealth command line interface (CLI)</td>
<td>Perform many of the same tasks that you can perform using the graphical user interfaces, as well as automate certain tasks by executing scripts.</td>
</tr>
</tbody>
</table>
| OneClick for eHealth console (OneClickEH) | - Perform policy-based discoveries of resources.  
- Manage polling errors.  
- Create and manage element groups and group lists.  
- Control user access to reports, administrative functions, elements, groups, Live Health applications, and Report Center.  
- Add and manage scheduled discover jobs, as well as modify scheduled default system jobs.  
- Create and manage Traffic Accountant views and groups. |
Chapter 2: Configuring the eHealth Administration User Interfaces

This chapter contains the following sections:

- The eHealth Console
- The OneClick for eHealth Console
- eHealth Command Line Interface
- The eHealth Web User Interface
- eHealth Product Licenses
- SSL Protocol

The eHealth Console

The eHealth console is a graphical user interface composed of menus and icons that provide access to key administration tasks such as managing standard eHealth reports, the database, and service profiles.

How to Access the eHealth Console on a Windows System

To open the eHealth console on a Windows system, log in as the eHealth administrator, and then click Start, Programs, eHealth versionNumber, eHealth. eHealth versionNumber is the default Program Group. Your Start program menu names may be different if you specified other names during the eHealth installation.

Open the eHealth Console on a UNIX System

To open the eHealth console on a UNIX system, you must log in as the eHealth administrator.
To open the eHealth console on a UNIX system

1. Enter the following in any terminal window (such as an xterm or shell window), where `eHealth` is the full directory pathname:
   
   ```
   cd eHealth
   ```
   
   The directory changes to the eHealth directory in which you have installed eHealth.

2. Do one of the following:
   a. Use one of these commands to source the appropriate `eHealth` resource file:

   Your environment is set.

   b. Change to the `/eHealth/bin` directory and enter the following command:

   ```
   eHealth
   ```
   
   The eHealth console appears.

Shut Down Your eHealth Console Windows Workstation

If you need to shut down your workstation, you must first stop eHealth and the database manager.

**Important!** Failure to stop either the eHealth server or the database manager before shutting down the workstation could corrupt the data in the eHealth database.

To shut down your Windows workstation

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:

   ```
   nhServer stop
   ```
   
   The eHealth server stops.

3. Select Console, Quit.

   The console closes.

4. Change to the following directory, where `eHealth` is the full pathname of the eHealth directory:

   ```
   cd eHealth
   ```
5. Enter the following command: 

```
./bin/nhStopDb
```

The database manager stops.

6. Shut down your workstation by following your standard system procedure.

**Shut Down Your eHealth Console UNIX Workstation**

If you need to shut down your workstation, you must first stop eHealth and the database manager.

**Important!** Failure to stop either the eHealth server or the database manager before shutting down the workstation could corrupt the data in the eHealth database.

**To shut down your UNIX workstation**

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:
   ```
   nhServer stop
   ```
   The eHealth server stops.
3. Select Console, Quit.
   The console stops.
4. Log in as the eHealth user by entering the following command and the account password:
   ```
   su eHealth
   ```
   The system logs you in.
5. Change to the `eHealth` directory in any terminal window (such as an xterm or shell window), by entering the following:
   ```
   cd eHealth/bin
   ```
   The system changes you to the eHealth directory.
6. Enter the following command:
   ```
   ./nhStopDb
   ```
   The database manager stops.
7. Log out of the eHealth user account, and perform a normal UNIX shutdown.
   Your eHealth system shuts down successfully.

**Display Alias Names**

By default, eHealth displays elements with the names that it creates when it discovers them. If these names are long and difficult to recognize, you can specify more meaningful alias names by modifying the element properties through the OneClickEH console manually or by importing them using DataSync. When you run or schedule a report, you can configure the report to use the alias
names instead of element names. If you set the Show Alias Names global option in the eHealth console, eHealth will display alias names when you view, edit, modify, or add elements.

Enable Time Zone Setting in Report User Interface

To provide eHealth reports that are customized for other time zones, you can specify a time zone for each report. When you generate a report and select a time zone, the report period reflects the time range in the report consumer’s time zone. By default, eHealth disables the ability to use time zones. To enable the option when you generate or schedule reports, you must select the Show Report Time Zones global setting in the Options menu. This setting applies to all reports.

When a user chooses a time zone for a report, eHealth does the following:

- Selects and displays data for the report appropriate for the time zone.
- Displays the time zone in the title and footer of the report.
- For scheduled reports, applies a GMT offset to the scheduled report runtime.

**Important!** Your operating system may not support all time zones. eHealth does not display unsupported time zones in its Time Zone list.

**To enable the global setting for time zones**

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Options.
   The Options dialog appears.
3. Select Show Report Time Zones, and click OK.
   eHealth applies this setting to all reports that you generate from the eHealth console and output to the Web user interface for viewing by users, and it also applies it to any reports that you schedule.

Set Date and Time Formats

If you want to change the format in which the date and time appear on the eHealth console, eHealth reports, and the eHealth web interface, you must change the NH_DATE_FMT and NH_TIME_FMT environment variables:

- **NH_DATE_FMT** specifies the format used for the date values in eHealth reports, the eHealth console, and the web interface. This variable is set to the format that you specify during the eHealth installation. If you change this variable after installation, the change affects only the date values in scheduled reports and the eHealth console.
- **NH_TIME_FMT** specifies the format used for the time values in eHealth reports, the eHealth console, and the web interface. This variable is set to the format that you specify during the eHealth installation.
Note: For a description of the values of these environment variables, see the eHealth Commands and Environment Variables Reference Guide.

If possible, refrain from changing the date or time on a Windows system, particularly on a temporary basis. If you must do so, stop the eHealth server first, change the date or time, and then restart the server. Your reports will show a gap in data while the server is stopped.

Important! If you have a Windows system and you need to change your system date or time when eHealth is running—even temporarily—use caution; this action can be particularly problematic. For example, if you move the month forward, eHealth uses that new time when recording any data that it polls during this temporary time change. If you exit the window by cancelling, thereby reverting to the previous time, eHealth tries to enter subsequent data earlier than your last entry. The database does not allow this action, so it results in errors until the current date/time exceeds the latest timestamp in the database.

The OneClick for eHealth Console

OneClick for eHealth (OneClickEH) is an additional administrative interface to the eHealth system that is automatically installed with eHealth. From this interface, you can monitor and manage your eHealth systems and view your element hierarchy. You can perform many administrative functions such as discovering resources, and managing elements, groups, scheduled jobs, and eHealth web user accounts.

The OneClickEH interface can manage multiple eHealth systems, even if they are mixed versions. OneClickEH supports eHealth Releases 6.1 and later, running on Sun, HP-UX, and Windows operating systems. The OneClickEH interface runs on Windows 2000, 2003, and XP operating systems; it is not supported on Windows NT and UNIX operating systems.

Important! To access the complete range of features available with OneClickEH, you must upgrade to eHealth r6.1.

Access the OneClickEH Console

OneClickEH is automatically installed with eHealth. When you launch eHealth, it displays the OneClickEH console next to the eHealth console (Windows eHealth servers only). You can also access OneClickEH by clicking the link on the Administration page of the Web user interface or by using the following procedure.

To access the OneClickEH console

1. Log in to the OneClickEH console by entering the following in a web browser:
   
   eHealthSystem/OneClickEH

   If your eHealth system is configured to run in a High Availability environment, specify the shared hostname or shared IP address (in v4 or v6 format) for your system rather than the specific eHealth system name.
The Connect to eHealth window appears.

2. Specify the user name and password of an administrator who has permission to access OneClickEH, and then click OK.

The OneClick for eHealth page appears.

3. Click Launch OneClick for eHealth.

The File Download window appears.

4. Click Run.

The OneClickEH login window appears. See *Set Up the OneClick for eHealth Console* for information about adding eHealth systems to your world view.

5. Log in to the eHealth system.

The eHealth Server Status page appears. This page provides a high-level status summary from which you can access more information by drilling down to various functions. A link at the top right side of the page lets you open the eHealth Web user interface in a new window.

**Note:** You can open the Server Status page outside of OCE by selecting eHealth Server Status from the Web Console. If you use this option, the Web Console link will not appear on the Server Status page.

---

**Set Up the OneClick for eHealth Console**

When the OneClick for eHealth console opens for the first time for a user, the world view is empty. To populate it, you must add one or more eHealth systems to it and log in to each one. You can add all of your eHealth systems to your World View, even if they are running on different platforms or supporting different eHealth releases. You can include a mixture of standalone eHealth systems, eHealth Distributed Systems, and eHealth Remote Poller or Traffic Accountant systems.

To log in to a system in your world view, you must enter a valid eHealth web user name and password for an account that has permission to access the OneClickEH console. By default, eHealth provides two web user accounts:

- **eHealth** - This account provides limited privileges for accessing the web interface, eHealth functionality, and reports. This is referred to as the web user account. By default, you cannot use this account to access any eHealth system that you add to your OneClickEH World View. To access an eHealth system using OneClickEH, an admin must modify the permissions on the account.

- **admin** - This account provides full administrative privileges to perform all functions through the eHealth web user interface and OneClickEH. This is referred to as the web administrator account.

**To add eHealth systems to your World View**

1. **Access the OneClickEH Console.**

2. Right-click the World View in the left-hand window of the OneClickEH console and select New Server.

3. After the new node appears in the tree, keep your cursor on it and specify a descriptive name for the eHealth system.
4. In the Login window, specify the name of your eHealth system in the Hostname/IP field. Use the fully-qualified domain name.
5. Specify a web port or accept the default; and specify either the HTTP or HTTPS protocol.
6. Specify the web administration user name and password in the appropriate fields.
   **Important!** OneClickEH requires you to enter a password to access an eHealth system. If the eHealth web user account does not have a password, you must modify the account and specify one.
7. Click Log In.
8. Add another eHealth system to your tree by repeating Steps 1 through 6.
9. Select File, Save World View.
   eHealth saves the file for future use.

**Preview Available OneClick for eHealth World Views**

If you have saved more than one World View, you can change views by right-clicking World View in the tree and selecting Load World View. You can also preview different World Views that you have saved before you load them.

If you attempt to load a new World View without saving the one that you have open, OneClickEH prompts you to save the open view before allowing you to apply a different one to your OneClickEH console.

**To preview other saved World Views before loading one:**

1. Access the OneClickEH Console.
2. Select Tools, Options in the menu bar.
   The Options dialog appears.
3. In the left pane, click the World View icon.
   The World View window appears.
4. Select your view location by doing one of the following:
   • From the Address list, select the pathname or URL of the World View to apply, or select the button next to the list and type in the location.
   • Select the address that appears in the list and replace it by specifying a new location.
   • Click the button to the right of the address list to browse for the view of your choice.
5. If the location that you select is password-protected, specify the authorization code in the HTTP Basic Auth field and specify your password.
6. Click Preview.
   The view appears in the Preview window.
7. Click Apply or OK to return to your OneClickEH console.
8. To return to your original World View, repeat Steps 2 through 7.
Organize Your World Views

If you have many eHealth systems supporting your business, you can organize your World View to make it easy to find each system quickly. For example, you can place your eHealth systems in a hierarchy of folders based on geographic region.

To add a folder to your World View tree

1. Access the OneClickEH Console and log in to the eHealth system.
2. Right-click World View in the tree and select New Folder.
3. After the new folder appears in the tree, keep your cursor on it and specify a descriptive name for the folder (for example, Boston).
4. Drag and drop one or more eHealth systems into the folder.

You can rename a folder or a system in your World View at any time by right-clicking the name in the tree.

Save the User Name and Password

By default, OneClickEH requires every user to supply a web user name and password to log in to an eHealth system. After a user logs in, OneClickEH displays a dialog to allow the user to save the login information. Once OneClickEH saves login information for a system, it automatically supplies the user name and password for every future login attempt. You can disable the automatic login and also prevent other users from being able to use it.

To disable the automatic login for an eHealth system

1. Access the OneClickEH Console.
2. Select Tools, Options, Advanced in the menu bar.
   The Advanced Settings window appears.
3. Deselect Log In Automatically to disable the automatic login.
4. (Optional) Clear all temporary objects that you have saved during your OneClickEH session.
5. Click OK.
6. Log out of the system and then log in again.
   OneClickEH should require you to supply the user name and password.

To hide the login save feature from all users

1. Open a command prompt window, and log in as the eHealth administrator to the system on which you have installed OneClickEH.
2. Change directories to eHealth/web/cmi.usr/config or the default directory for OneClickEH.
3. Create a file named cmi.ini within that directory.
4. Add the following text to the file:

   server-options=[HIDE_REMEMBER_LOGIN]

5. Save and close the file.

   OneClickEH hides the user name and password prompts in the Advanced Settings window and no longer prompts the user to save the login information after every login attempt.

### eHealth Command Line Interface

eHealth provides commands that you can run from a console or terminal window to perform basic or advanced administrative functions, and to automate tasks. Most of the basic command functions are also available through one of the administrative interfaces.

### How to Use the Command Line Interface

You can run any eHealth command from any drive on the system on which you have installed eHealth. Before running a command, however, you should review the usage to verify the purpose and syntax.

**To use the command line interface**

1. Log in to the eHealth system and select Start, Programs, Accessories, Command Prompt.
   
   A command prompt window appears.

2. Enter the following to change to the drive on which you have installed eHealth, and then press Enter:

   `driveNumber:`

   The prompt changes to the specified drive.

3. Change to the directory that contains the eHealth command line interface:

   `/eHealth/bin`

4. Enter the following to list all available commands:

   `ls`

   The list of commands contained in the bin directory appears.

5. Scroll through the list to find the command that you want to use, and then enter the following to review the syntax of a command:

   `commandName -h`

6. Run the command with the appropriate arguments.

   eHealth displays the output for the command.
Important! Some commands are specifically intended for use only under the direction of Technical Support. If a command is not documented in the eHealth Commands and Environment Variables Reference Guide, do not use it unless directed to do so by Technical Support.

The eHealth Web User Interface

eHealth installs a web server to enable users to view eHealth reports and other features from any remote system using a web browser. From the various tabs of the web interface, you can perform administrative functions, generate eHealth reports, and access numerous eHealth products. eHealth automatically installs the Apache web server and software to allow you to view reports from a web browser. To access the eHealth web server, specify the server’s uniform resource locator (URL) in a web browser by using one of the formats specified this table. If you are unable to access the web server, see eHealth Web Server Is Inaccessible on a UNIX System on page 274 for troubleshooting instructions.

Log In to the eHealth Web User Interface

When you access the web server, eHealth displays a welcome page and the message of the day. If web security is enabled on your system, the system requires you to supply the user name and password associated with your eHealth web user account. If you have not already done so, ask the eHealth web administrator to create a web user account for you.

To log in to the eHealth system

1. Do one of the following:
   - Access the OneClickEH Console, log in to the eHealth system, and select the eHealth Web UI link in the left pane of the console.
   - Specify one of the following URLs in a web browser:

<table>
<thead>
<tr>
<th>URL Format</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://ipAddress">http://ipAddress</a></td>
<td>For IP address, specify the IP address (in v4 or v6 format) of the eHealth system.</td>
</tr>
</tbody>
</table>
2. Click Continue.
   The Enter Network Password dialog appears.
3. Enter your eHealth web user name and password, and click OK.
   The eHealth web user interface appears.
4. Select a tab in the navigation bar.
   The specified page appears.
5. If a particular tab does not appear in the navigation bar, ask an admin to confirm that your user account has permission to access that page.

### Unauthenticated (Open) Access to the Web User Interface

By default, eHealth enables web security to require all users to provide a valid user name and password to access the Web user interface. On the Site Configuration window on the Administration page, you can disable web security for the entire eHealth site. When you disable web security for an eHealth site, you essentially grant all users unauthenticated access to the Web user interface.

After you disable web security, the following occurs:

- Each user who accesses the eHealth web server automatically has unauthenticated (open) access to the eHealth Web user interface.
- The eHealth system automatically logs in every user as the web user named public.
- All users, including the web administrator, use this public user account when viewing and generating reports.
- If you modify the permissions associated with the public user account, your changes affect every user.
You cannot modify the access permissions for individual users. To apply different access permissions to individual users, you must enable web security for the eHealth site to require each user to log in to the system as a web user, and then modify the permissions on the individual accounts accordingly.

To access administrative functions, you must select Authorized Access on the Administration page and specify a web administrator user name and password.

**Important!** When you re-enable web security, the system requires any users who are currently accessing the web server to specify a web user name and password the next time that they want to perform a function through the Web user interface.

**LDAP Authentication for eHealth**

You can set up the eHealth Web Server for Lightweight Directory Access Protocol (LDAP) authentication by configuring eHealth for Single Sign-On (SSO) support. SSO support requires the CA EEM server to be installed on a separate system. Once the CA EEM server is installed, you can configure the CA EEM server to authenticate using LDAP. To provide LDAP authentication support for an eHealth-only environment, you can run the nhWebSso command to enable SSO.

**Note:** For instructions on enabling LDAP authentication, see the *eHealth Installation Guide*. For instructions on running the nhWebSso command, see the *eHealth Commands and Environment Variables Reference Guide*.

**eHealth Product Licenses**

eHealth licenses control the features that you use and the number of elements that you monitor. The specific eHealth licenses that you should purchase for your organization depend on the number and types of resources that you want to monitor. Before you can use licensed eHealth products, you must obtain authorized license keys for your eHealth software products. From the OneClickEH console, you can track your license status and usage.

**Track License Status and Usage**

To enable eHealth to continue to poll all of your resources, you track the status of your eHealth product licenses from the OneClickEH console.
The License Tracking feature of the OneClickEH eHealth Status Summary provides an overview of your license consumption. It itemizes the total number of licenses that are available to poll elements, the number that you have purchased, and the total number that you need to monitor all of your discovered elements. If you have very few licenses available or have run out of licenses, you can use the License Keys feature to review all of the licenses that you have purchased.

**To track license status and usage**

1. [Access the OneClickEH Console](#) and log in to the eHealth system as a web user who has permission to view system information.
2. Log in to the eHealth system.
   - The eHealth Status Summary window appears.
3. In the left pane of the console, select Tasks and Information, System Information, and then double-click License Keys.
   - The License Keys window appears.
4. Do the following:
   a. Click the Expiration column to identify how many licenses will expire soon.
      - The table reorders the data based on date.
   b. Scroll through the License Keys table to review the data.
      - **Important!** If you spend a significant amount of time reviewing the data, right-click and select Refresh Data (or press F5) to update the table with the latest data.
   c. (Optional) Right-click, select Export All, and specify a file name.
      - eHealth saves the data to a file.

To make more licenses available, you can free licenses that are being used by elements that you are not currently monitoring. For instructions, see [Redistribute Polling Licenses on page 68](#).

**How to Add eHealth Licenses**

Before you can use licensed eHealth products, you must request authorized license keys for your eHealth software products. To obtain the keys, you must submit a request through the Technical Support web site. The Licensing department of CA will provide you with specific information about each poller license and product licenses that you have purchased. To add more poller licenses or a new eHealth product license, you need to obtain an updated set of license keys from the Licensing department by following the exact same process.

**To add one or more eHealth licenses to eHealth on a Windows system**

1. Log in to http://ca.com/support.
   - The Technical Support page appears.
2. Select the licensing tab.
The Licensing page appears.

3. Click on eHealth Network License Request Form, complete the fields, and click Submit.

   The Licensing department sends you a set of authorized product keys.

4. Create a backup of the license.dat file that resides in the $eHealth/lmgr$ directory.

5. Open the license.dat file that resides in the $eHealth/lmgr$ directory.

6. Open the e-mail message that Licensing sent to you.

7. Copy and paste only the license keys from the message into the file to overwrite the existing entries. Do not include the e-mail header information.

   **Important!** If you include the e-mail header information, the license will not function correctly.

8. Save the file and close it.

9. Do one of the following:

   - If you added or changed your poller license keys only, enter the following at the command line on a Windows or UNIX system:
     
     ```
     nhupdateLicenses
     
     eHealth reloads the license.dat file without restarting the eHealth system.
     ```

   - If you added or changed non-poller license keys, select Start, Control Panel, Administrative Tools, Services, and then restart your eHealth system and FlexLM Manager services on your Windows system.
     
     eHealth restarts the processes and enables your licenses.

   - If you added or changed non-poller license keys, restart your license manager on your UNIX system. Enter the following:
     
     ```
     cd $eHealth/bin
     
     nhLmgr stop
     nhLmgr start
     
     eHealth restarts the license manager and enables your licenses.
     ```

**How to Move eHealth Product Licenses from One Workstation to Another**

If you have more than one eHealth workstation, you may need to move license keys from one workstation to another (for example, when upgrading to a larger server). To move license keys, you must complete the appropriate licensing form through the Technical Support web site.

**To move eHealth licenses from one eHealth system to another**

   
   The Technical Support page appears.

2. Select the licensing tab.
   
   The Licensing page appears.

3. Click on eHealth Network License Change Request Form, complete the fields, and click Submit.
The Licensing team sends you a set of authorized product license keys for the designated eHealth system.

SSL Protocol

If your organization requires secured communication within the eHealth web application, you can apply the Secure Sockets Layer (SSL) protocol (HTTPS) to your eHealth web server.

SSL is the standard protocol for encrypting information transmitted between a web site (server) and browser (application interface), and is supported by Internet Explorer and Firefox. Web sites use SSL to securely transfer confidential user data (for example, a user’s credit card number or eHealth user account information). SSL-encrypted data is private and protected from tampering or eavesdropping. The SSL public and private key encryption system uses a secure server certificate to secure communication.

SSL in the eHealth Environment

To maintain privacy and encrypt all communication between the eHealth web server and eHealth clients, you must enable SSL on the eHealth web server. SSL prevents data owned by one user from ever being seen by other users and does not allow sensitive data to be revealed to third parties. When implemented properly, SSL provides the following security features:

- Proof that the server is legitimate and trustworthy.
- Different levels of data encryption.

SSL affects all eHealth applications that communicate through the web server, including the following applications:

- eHealth web clients
- SPECTRUM web services
- Report Center Interface
- OneClick for eHealth console
- Business Service Console
- Live Health - Live Trend, Live Exceptions, and Live Status

SSL can be enabled on web servers in Distributed, Remote Poller, and High Availability environments.
SSL Components

The following components work together with eHealth to properly enable SSL:

- **Secure Server Certificate.** To generate an SSL connection, a web server requires a secure server certificate, either self-signed or issued through a Certificate Authority. Secure server certificates electronically establish a server's credentials when doing business on the Internet or performing other online or electronic transactions. These certificates include a serial number, expiration date, a digital signature of the Certificate Authority, and a copy of the certificate holder's public key.

- **nhWebProtocol Command.** A command-line interface utility is installed with eHealth. Use the nhWebProtocol command and its arguments to enable and disable SSL on your eHealth systems. For a full description of this command, its syntax and arguments, see the eHealth Help.

- **Apache 2.2.** Apache web server version 2.2 is installed with eHealth r6.1 and supports SSL.

- **OpenSSL.** OpenSSL is a self-signed secure server certificate generation program installed with eHealth r6.1. OpenSSL is located in the `eHealth/web/httpd/bin/openssl` directory.

How to Enable SSL on Your eHealth System

Enable SSL on your eHealth system and complete the following tasks:

- Install eHealth r6.1 on your system.
- Generate a private key and a certificate signing request pair.
- Purchase a secure server certificate issued through a Certificate Authority such as VeriSign or GeoTrust for each eHealth server that you want to secure with SSL.
- Enable SSL on your eHealth servers.

To avoid problems when you enable SSL in your environment, follow these general guidelines:

- Configure SSL on all supported eHealth platforms: Windows, Solaris, and HP-UX.
- Do not use self-signed certificates in your production environment. Use them only in a lab to test SSL without the expense and time involved in purchasing a certificate from a Certificate Authority.

Generate a Private Key and Certificate Signing Request

Before you purchase a secure server certificate from a Certificate Authority, you must first generate a private key and a certificate signing request (CSR) from the Certificate Authority for the eHealth server on which the certificate will be installed. The CSR acts as your public key.
Important! The procedure provided in this guide is a guideline; you must use the procedure provided by your Certificate Authority. The procedure must be specific to Apache mod_SSL. If you currently run eHealth with a custom SSL-enabled web server, you must follow the procedures in this guide as they are specific to eHealth and use components installed with eHealth r6.1 and later.

Many Certificate Authorities now issue intermediate Certificate Authority certificates. Installing both certificates on your system creates what is known as a trust chain that starts at a trusted Certificate Authority, continues through the intermediate certificate, and ends with the secure server certificate. This chain enhances the security of your certificate.

To generate a private key and CSR

1. Log in to the eHealth system as an administrator and open a command prompt window.
2. Navigate to the following directory: `/eHealth/web/httpd/bin`
3. Enter the following command to generate a 1024-bit private key:
   ```bash
   openssl genrsa -des3 -out www.hn.com.key 1024
   ```
   where `hn` is the fully-qualified eHealth system hostname. The key is stored in the file `www.hn.com.key` and will be used to generate the CSR.
   
   **Important!** Each time that you connect to the web server, you will be prompted for a pass phrase that will be encrypted in the private key unless you use the `-passphrase` argument when you run the `nhWebProtocol` command. The pass phrase requires a minimum length of 4 characters; space characters should not be used.

   ```bash
   ```
   where `hn` is the eHealth system hostname.
4. Enter the following command to generate the CSR:
   ```bash
   ```
   where `hn` is the eHealth system hostname.
5. When prompted, answer questions regarding any additional information that you want to associate with the CSR.

   After the Certificate Authority verifies and processes this request, it will send you the signed certificate, which acts as your public key. If required, you will also receive the intermediate CA certificate.

Enable SSL

You can enable SSL support in your eHealth network with a secure server certificate, either self-signed or issued through a Certificate Authority. You enable SSL by using the `nhWebProtocol` command. For the complete syntax of this command, see the eHealth Help.
To enable SSL using a signed certificate from a Certificate Authority

1. Log in to the eHealth system as an administrator, and open a command prompt window.
2. Enter the following command:
   
   ```
   nhWebProtocol -mode https -port portNumber -certificate certificatefile -key keyfile -intermediate intermediateCertificateFile -passphrase 1234
   ```

   where `portNumber` is the custom port for the web server, `certificatefile` is your digital identity certificate (the public key), `keyfile` is the key associated with the certificate, `intermediateCertificateFile` is an intermediate certificate issued by a Certificate Authority for another Certificate Authority (include this if you were issued an intermediate certificate), and `1234` is the pass phrase you entered when you generated the private key (include this if you entered a pass phrase when you generated the private key).

   This command performs the following tasks:
   - Copies the certificate and key files into `eHealth/web/http`.
   - Sets the web server state to SSL-enabled.
   - Configures the Apache web server for SSL.

To enable SSL using a self-signed certificate

1. Log in to the eHealth system as an administrator, and open a command prompt window.
2. Enter the following command:

   ```
   nhWebProtocol -mode https -port portNumber -hostname hostname
   ```

   where `hostname` is the fully-qualified hostname of the eHealth system on which you want to enable SSL, and `-port` is an optional value that specifies a value used to map data through a network protocol to a particular process.

   This command performs the following tasks:
   - Generates a self-signed certificate and corresponding key.
   - Copies the files into `eHealth/web/http`.
   - Sets the web server state to SSL-enabled.
   - Configures the Apache web server for SSL.

Disable SSL

EHealth gives you the ability to disable SSL support. This is useful if you want to restore the default (HTTP) web server configuration to troubleshoot problems encountered when implementing SSL.

To disable SSL

1. Log in to the eHealth system as an administrator, and open a command prompt window.
2. Enter the following command:

```
nhWebProtocol -mode http -port portNumber
```

- `port` is an optional value that specifies a value used to map data through a network protocol to a particular process. If you do not specify `-port`, eHealth uses the default port (80).

This command performs the following tasks:
- Sets the web server state to normal security (non-SSL).
- Configures the Apache web server and resets the port number.

---

### Add a Self-Signed Certificate to the Live Health Client

If the Live Health applications in your test environment communicate with servers enabled with a self-signed certificate, the certificate must be added to the system’s Java Runtime Environment (JRE) keystore.

**To add a self-signed certificate to the Live Health keystore**

1. If you have not done so already, log in to your eHealth system and change the NH_HTTP_PORT environment variable to 443 (to correspond to the port that you configured for the eHealth Web user interface on which you enabled SSL support); then restart the eHealth system.
2. Log in to the eHealth Web user interface that is enabled with a self-signed certificate, click the Live Health tab, and download the Live Health installation package.
3. When the system prompts you to do so, accept the self-signed certificate. The certificate appears.
4. View the certificate and note the fully-qualified name of the eHealth server to which the certificate is issued. You *must* provide the exact name as it appears on the certificate to log in to the Live Health applications.
   **Important!** In the certificate, CA refers to the Certified Authority certificate file in the keystore. It is not a reference to CA (Computer Associates).
5. Copy the certificate file (.crt) located in the `eHealth/web/httpd/conf` directory and save it to a $TEMP directory.
6. Install Live Health. For instructions, see the eHealth Help.
7. Open a command prompt window.
8. Import the self-signed certificate into the keystore (a file that contains both keys) by selecting one of the following options depending on your environment configuration:
   - If you have one eHealth server in your environment:
     a. Enter the following command:

     ```
     $LH_HOME/client/jre/bin/keytool -import -file
     $TEMP/certificatefile.crt -keystore
     $LH_HOME/client/jre/lib/security/cacerts
     
     where cacerts is the default keystore for the JRE.
     ```
b. Enter the following password:

   changeit

   where changeit is the default password for the keystore.

c. Accept the self-signed certificate after verifying that it is issued to
   the correct server name, as noted in Step 3.

If you have multiple eHealth servers in your environment (for example, multiple eHealth clusters are managed from one Live Health client) and you are adding multiple certificates, do the following:

a. Enter the following command:

   Note: When you use self-signed certificates in an eHealth cluster
   environment, or you expect Live Health clients to connect to multiple
   eHealth web servers using a secure connection, you must import the
   certificate from each eHealth web server to the keystore of each Live
   Health system. To do this, you provide an alias for each certificate
   you import. For example, the first certificate might be AliasOne, the
   second certificate would be AliasTwo, and so on.

   $LH_HOME/client/jre/bin/keytool -import -file $TEMP/certificatefile.crt
   -keystore $LH_HOME/client/jre/lib/security/cacerts -alias alias

   where alias is the alias name for the certificate and cacerts is the
   default keystore for the JRE.

b. Enter the following password:

   changeit

   where changeit is the default password for the keystore.

c. Accept the self-signed certificate after verifying that it is issued to
   the correct server name, as noted in Step 3.

d. Repeat steps a-c until you have imported all certificates.

9. When you start Live Health, click the User tab and supply the server name
   noted in Step 2 when the system prompts you to do so.

   Important! Do not provide the IP address of the server during this
   procedure. If the certificate configured on Live Health applications does not
   match the one used for the server, Live Health will not run properly.

10. Click the Network tab and check the Use Secure Connection box, then click
    OK.

    The Live Health clients are configured to use SSL.
Chapter 3: Discovering Resources

This chapter contains the following sections:

- eHealth Discovery
- Discover Log File
- Rediscovery
- Community Strings
- Scheduled Discover Job

eHealth Discovery

eHealth discovery is the process by which eHealth locates resources within your infrastructure so that it can collect data from them and report on their performance and availability. Depending on the licenses that you have purchased, eHealth is able to discover different types of resources within your infrastructure and create elements for them. After eHealth discovers a resource, it adds it as an element—its representation of your business resource—to the database.

Discover Methods

As an eHealth user, you typically discover the resources within your infrastructure using the interactive discover feature which is available through the OneClick for eHealth console user interface. From that user interface, you can also schedule discover jobs to run on a regular basis.

In addition, eHealth offers these other discovery methods as alternatives:

- The DataSync Application Programming Interface – This interface enables you to import element information from sites that have a network management system (NMS) or other source that collects configuration information and data for resources. To use DataSync successfully, you must have a working knowledge of eHealth and be comfortable creating programs, scripts, and files that use complex syntax. For detailed instructions, see the eHealth Integration Guide.
The *eHealth Command Line Interface* – This interface enables you to run a command to perform an interactive or scheduled discovery. The nhDiscover command, which resides in the *ehealth/bin* directory, has the same features that are available through the OneClickEH console. For detailed information about using this utility, see the *eHealth Commands and Environment Variables Reference Guide*.

### How eHealth Discovers Resources

To monitor and manage the performance of the network, eHealth uses the process of discovery to locate resources within the infrastructure.

To discover resources within a network, eHealth does the following:

1. Uses Simple Network Management Protocol (SNMP) agents to search particular ports for the IP addresses that you specify.
2. Obtains information from the management information base (MIB) of each device and creates elements based on that information.
3. Stores the element information in its database.

### How to Identify Your Infrastructure Resources

Your infrastructure typically contains resources such as routers, systems, switches, probes, modems, and other devices. These resources contain interfaces that connect them to each other and form the topology of the infrastructure. Users connect to various systems over the topology to access critical applications. Before you perform an eHealth discovery, identify the specific resources that you want to monitor within the infrastructure.

To identify your infrastructure resources, do the following:

1. Consult a network or system administrator to obtain a map or a list of the devices in your infrastructure.
2. Create a list of IP addresses in an electronic file for future reference. You can use v4 or v6 format.
3. Identify any resources that you do not need to monitor at this time.
4. Distinguish between a physical element and a logical element:
   - A physical element is a device or component such as a specific port on a specific card of a specific router, for which discover collects data, regardless of who uses it or why.
   - A logical element is a device or component for which eHealth reports on its logical purpose. For example, if a link from New York to Boston moves from one router to another router, you would want eHealth to retain the data for the element from the previous device and collect the new data from the new device.
5. Identify the ports that you want eHealth to search. By default, eHealth looks for SNMP agents at port 161, but it also looks for system agents at ports 1691 and 6665. If you want eHealth to search for SNMP agents on other ports, you can set one of the following parameters when you create your Discover Policy:
   - Ports - Application specifies the agent ports for application service elements.
   - Ports - System specifies the agent ports for system elements.
   - Ports - All specifies the agent ports for all elements.
   - Ports - Response specifies the agent ports for response elements.

How to Discover Resources Interactively

As a best practice, when you run the discover process for the first time, use an interactive discover rather than scheduling the task. Before discover saves the elements that it finds, eHealth gives you the opportunity to edit the results. This allows you to control the resources that it will poll within your infrastructure.

To perform an initial discovery, follow these steps:

1. Confirm that your eHealth web user account has permission to perform discoveries.
2. Access the OneClickEH Console and then log in to your eHealth system.
3. Create a Discover Policy.
4. Specify the IP addresses and other settings, select the Discover Policy, and run the discover.
5. Review the discover results.
6. Edit the results, if necessary, and save the element data to the eHealth database.

Create a Discover Policy

In a Discover Policy, you specify the types of devices that you would like to find and specific configuration parameters associated with the element type that you want to monitor. Before you perform an interactive discovery or schedule a discover job to run, you can create new discover policies on-the-fly by using the OneClick for eHealth console.

To create a Discover Policy

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth system.
2. In the left pane, select Tasks and Information, Resource Discovery, Policies.
3. Right-click and select New Policy.
   The Create Discover Policy window appears.
4. Specify a name.
5. (Optional) Specify a description to distinguish this policy from others that may have a similar name.

6. (Optional) From the Technologies list, select the types of resources that you want to discover. (You can also specify the technology type when you run the interactive discovery.)
   - If you selected System as the technology type, select Use Process Sets to track the impact of individual processes for the applications that are running on the system. For more information on this option, see Collect Data from System Elements on page 174.
   - If you selected LAN/WAN as the technology type, select Find MIB2 LANs to limit the discovery to LAN interfaces that support basic MIB2 statistics such as In/Out/Total packets. For more information about this option, see Limit the Discovery of LANs on page 48.

7. (Optional) Select a DCI rule that you want eHealth to use to filter your discover. For instructions on creating a DCI rule, see Use a DCI Rule to Include or Exclude Elements on page 49.

8. (Optional) If you want eHealth to save elements to one or more existing groups, specify those groups. Use commas to separate the group names. To search for a group name, specify part of the name in the field, and then press Enter to display a list of up to 50 matching groups.

9. After the parameter table displays the discover parameters that support the selected technologies, review the parameter list, and do one of the following:
   - Import the parameter settings from a pre-r6.1 discover job. Click Populate from scheduled job.
   - Accept the default parameters. If necessary, modify the parameter values by clicking on each parameter row and then clicking Edit. Specify a different value and click OK.

10. Click OK at the top of the Create Discover Policy window.

**Import Discover Policies from One eHealth System to Another**

If you want to use the same discover policies to run discoveries on different eHealth machines, you do not have to recreate the Discover Policy on each machine. To save time, you can use a command line utility to export your discover policies from one eHealth system, and then import the policy data into the eHealth database of another eHealth system.

**To create a Discover Policy using the command line interface**

1. As an administrator, log in to the eHealth system that contains the discover policies that you want to export.
2. Open a command prompt window.
3. At the command line, run the following command:
   ```bash
nhDiscoverPolicy -export
eHealth generates two XML files that contain the policy data.
4. Using FTP, move the XML files to the target machine.
5. On the target machine, at the command line, run the following command:
   `nhDiscoverPolicy -import`
   eHealth copies the policy data into the eHealth database.
6. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage discoveries.
7. In the left pane, select Tasks and Information, Resource Discovery, Policies.
   The Discover Policies should now appear in the Policies list in the right window.
   **Note:** For the complete syntax of the `nhDiscoverPolicy` command, see the [eHealth Commands and Environment Variables Reference Guide](#).

### Run an Interactive Discover

If you have not used eHealth to discover resources within your infrastructure before, you need to run an interactive discover. Based on the technologies that you specified in the Discover Policy, eHealth discovers different types of resources within your infrastructure and uses various methods to create elements for them. For each resource that eHealth discovers, the method by which it creates a corresponding element varies. For details on the different ways that eHealth discovers each resource type, see [Appendix B: eHealth Element Naming Conventions](#).

### To run the discover process interactively for the first time

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth system.
2. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
   The Discover window appears.
3. Select the Options tab.
4. Specify the IP addresses for which eHealth should search. You can use v4 or v6 format. Specify a pre-existing IP address exclusion file, or create a file that contains the following:
   - An inclusive range. Separate the first and last number with a dash, specify a single IP subnet, specify a range between 0 and 255, and do not insert spaces. For example, 128.12.10-12.87 searches for 128.12.10.87, 128.12.11.87, 128.12.12.87.
   - A list of specific numbers separated by commas, but without spaces. For example, 128.12.5,19,22.87 searches for 128.12.5.87, 128.12.19.87, 128.12.22.87.
5. Select the policy name and specify a community string.
6. (Optional) Select a technology if your Discover Policy does not include a specified technology, or if you want to override the technology setting specified in the Discover Policy.
7. Click Discover to start the discover process.

   The Discover progress dialog displays the following details concerning the progress of the discovery:
   - The number of elements that it found, the number of missing elements, and the number of elements that it updated
   - Devices that did not respond to ping
   - SNMP agents that it does and does not support
   - Broadcast addresses that it ignored because eHealth is unable to discover at that location
   - Addresses that it ignored because they are included in an IP exclusion file
   - Addresses at which an SNMP request timed out before the agent responded to the request
   - Addresses to which the SNMP agent responded with an error or with an indication that it expects a different community string or port number

8. Carefully review the discovered data and do one of the following:
   - If you do not want to retain any of the discovered data, click the X in the Discover Results dialog to discard the new elements without adding them to the database. eHealth then saves the log file as discoverInteractive.date.time.unsaved.log.
   - If you want to monitor all new elements that discover found, click Save Results in the Discover window. eHealth creates an entry in the database for each new element and saves the results in the pollerAudit.date.time.log file in the eHealth/log directory. After you save the results, eHealth immediately starts to poll the elements.
   - If you want to modify the configuration, select the Edit Results tab. Delete specific elements that you do not want to monitor or disable polling for them.

How eHealth Creates a Modem Pool Element

To report on modem pools that might span one or more RAS devices, you can discover devices using the Modem Pool technology.

To create a modem pool element, eHealth does the following:
1. Searches the specified IP addresses for RAS devices.
2. Creates an element for each of the following:
   - Each modem pool configured at the device
   - Each modem in the device
   - Each ISDN interface in the device
3. If the RAS device agent does not have a modem pool definition, creates a single modem pool element for the RAS device and assigns all modem and ISDN elements in the device to it.
4. Combines the total data collected for each modem and ISDN element in the pool to report on the health of the modem pool.
Discover Log File

When you run a discover process, eHealth compares attributes of the discovered elements to attributes of previously discovered elements. To resolve changes, discover uses a complex matching process based on discover keys. For an in-depth discussion, see Appendix A: The Discover Algorithm.

For each discover that you run, eHealth records the results in comparison to the existing database in a file named discoverInteractive.<date>.<time>.log. As a best practice, you should review the discover logs to identify the changes that eHealth has found within the infrastructure and determine the steps that you need to follow to update your database, if necessary.

To access the log files

1. In the left pane of the OneClick for eHealth console, select Tasks and Information, Resource Discovery, Interactive Discover.
2. In the Discover window, select the Log Files tab.
3. Scroll through the list of logs, select that one that you want to view, and click View Log.

Each discover log file displays a header composed of three sections: Discover Results, Network Change Summary, and Duplicate Analysis. The log includes the infrastructure changes that the discover process could resolve using existing information in the database. Discover is able to resolve an infrastructure change when it can update the database with the information without duplicating an element or incorrectly changing existing information.

Depending on the technologies that you select, eHealth discovers different types of resources within your infrastructure and uses various methods to create elements for them. For each resource that eHealth discovers, the method by which it creates a corresponding element varies. To interpret your discover results correctly, it is important to understand the different ways that eHealth discovers each resource type. For a detailed discussion, see Appendix B: eHealth Element Naming Conventions.

Discover Results Section

The Discover Results section of the discover log lists the time at which the discover occurred, indicates whether it was scheduled or interactive, and itemizes the options that you specified for the discovery.

Network Change Summary Section

The Network Change Summary section of the discover log identifies several types of elements: new, updated, unchanged, and missing. It also lists discover key changes—the unique identifiers that eHealth uses to recognize elements.
Duplicate Analysis Section

The Duplicate Analysis section of the discover log lists the number of suspected duplicate elements, duplicate (identical) names, and duplicate keys identified in the database. To avoid taxing your eHealth server, routinely resolve all duplicates and avoid rediscovering them in the future.

Discover Log Contents

The log records one or more of the following types of elements:

New Element

A device that discover locates within the infrastructure, but it is not in your current database.

Unchanged Element

A device that discover locates within the infrastructure, but its attributes have not changed in any way. The element still exists in your infrastructure, and discover did not detect any new configuration information.

Updated Element

A device that discover locates within your infrastructure, but its configuration information has changed. For example, discover would label a device (router, system, or RAS device) as updated if you replaced one piece of hardware with another, causing a change to the hardware ID. The discover process can resolve this change if you removed the old device from the infrastructure and made sure that the new device uses the same system name (sysName) and IP address as the old device.

Missing Element

A device whose IP address and UDP port fall within the discover process range, but discover was not able to find it for any of the following reasons:

- Discover request timed out before it could get a response.
- SNMP agent on the device is down (and, therefore, is unable to collect data from the device).
- Element no longer exists in the infrastructure.
- UDP port on which the agent is running has changed.

Important! If some, but not all, element properties change, eHealth may identify it as a new element and a missing element.

Duplicate Key

An element that discover finds within the infrastructure that has the same discover key as another element in the database. Discover identifies an element as a duplicate key if it has the same ifDescr variable across many interfaces in the device.
Suspected Duplicate Element

A device that discover finds within the infrastructure that appears to duplicate another element in the database. The element duplicates some attributes of another element that are normally used to identify it uniquely; or, the physical address or discover keys match, but the MIB indexes and MTF are different. If these elements are, in fact, duplicates, eHealth may be polling the same element twice.

Duplicate Element Name

A device that discover finds within the infrastructure that has the exact same name as another element in the database, but has one or more attributes that do not match. This could occur if the element’s system name, hardware ID, discover key, or agent type is not unique in the infrastructure, or the interface was replaced with another type. This could also occur if you specified the element name incorrectly when you modified it previously.

Resolved Updates

A change that discover makes to an element when it positively matches the element to another element in your infrastructure based on the discover key or physical address. When you save your discover results, it updates your database with the changed information. In general, eHealth can resolve the following infrastructure changes:

- New devices and components added to the network
- SNMP index shifts for elements with unique discover keys or unique MAC addresses
- One of the following changes to the attributes of a device:
  - Replacement of a chassis
  - Change to the IP address
  - Change to the sysName MIB variable of a device
  - Removal or addition of device components such as cards, memory, or disks
- Change to component attributes, except for changes to attributes used to create a discover key or to compare unkeyed components.
- Total device replacement

Unresolved Updates

A change that discover makes to an element after it matches it on the MIB index and MTF (which is a less reliable attribute), but is unable to match the element based on a discover key or physical address. In a case in which discover cannot resolve the change (that is, it cannot clearly discern the exact change to make to the database), it lists the change as unresolved to give you the opportunity to edit the element and avoid losing historical data or inadvertently creating multiple elements for the same resources.
How to Resolve a Missing Element

If missing elements are included in the Network Change Summary section of the log, scroll to the Missing Elements section. Determine how long the elements have been missing by examining the Missing Elements section of discover logs for previous days. If the elements have not responded for several days and you can verify that the elements have been removed, delete or retire them.

To resolve a missing element that no longer exists, follow these steps:

1. Access the OneClickEH Console as a web user who has permission to manage elements, and then log in to your eHealth system.

2. Do one of the following:
   - If you no longer want to report on the element, delete it.
   - If you want to continue to run reports on the element, retire it.

3. Delete it from any discovery IP address list file that you specify in your discoveries.

How to Resolve a Duplicate Key

If duplicate keys are included in the Duplicate Analysis section of the log, resolve them as soon as possible to prevent eHealth from rediscovering them again during future discoveries.

To resolve duplicate keys, follow these steps:

1. Update the device’s configuration to make sure that the ifDescr for the interface is unique on the device.

2. Rediscover.

How to Resolve a Duplicate Element Name

If duplicate element names are included in the Duplicate Analysis section of the log, resolve them as soon as possible to prevent eHealth from rediscovering them during future discoveries. If you leave them as is, discover will display them with a -A and -B suffix. For example: east-SH, east-SH-A, east-SH-B.

To resolve duplicate element names, follow these steps:

1. Access the OneClickEH Console as a web user who has permission to manage elements, and then log in to your eHealth system.

2. Find the duplicate elements in the element list.

3. Do one of the following:
   - Specify a new name for one of the elements.
   - Delete the duplicate.

Important! In some cases, discover identifies elements of similar agent types as duplicates because they share similar properties, but they are not truly duplicates. Use caution when deleting them. If you know that two elements are actually duplicates, delete the true duplicate. Otherwise, contact Technical Support for assistance.
How to Address Unresolved Updates

When discover is unable to match an element based on a discover key or physical address, it lists it as an unresolved update. It is important to address each unresolved update that appears in the log by identifying the reason that discover was not able to resolve the change. In most cases, you will need to modify the current database, and then run the discover process again to add the new or updated information to the database.

To address unresolved updates, do any of the following:

- Identify any components that you moved, removed, or replaced. Delete or retire the old elements.
- Identify any components that you redefined by changing the ifDescr MIB variable. Delete or retire the old elements.
- Identify any devices that were rebooted during a discovery. Modify the element properties to correct any resulting SNMP index shifts.
- Determine if you used the same ifDescr MIB variable for more than one ifTable entry. Modify element properties to eliminate any duplications.

If you are unable to determine why discover was not able to resolve one or more changes, see Unresolved Updates on page 45 for guidelines.

Rediscovery

Rediscovery is the process of running a discover to update your database after your elements have changed. If you rediscover often, as changes occur, you can maintain continuous data collection and significantly reduce the number of resource changes that discover is unable to reconcile based on current information in the database.

Important! Rediscovering a large number of elements can impact your system performance. To avoid performance problems, do not run multiple discover jobs simultaneously, and wait a few minutes before starting a new job.

Rediscovery is especially useful after you do any of the following:

- Upgrade to a new release of eHealth.
- Upgrade a device.
- Change the configuration of a device.
- Discover router/switch elements (to include router/switch interface elements in your LAN/WAN reports)
- Reboot a device.
How to Tailor Your Discovery

To run an interactive discovery, you must specify the IP addresses for the resources that you want to find. Over an extended period, you may determine that eHealth repeatedly discovers elements that you do not want to add to your database. As a best practice, enable eHealth to find the elements that you want to monitor by using these methods to tailor your discovery:

- **Limit the Discovery of LANs.**
- **Use a DCI Rule to Include or Exclude Elements.**
- **Search for Specific IP Addresses.**
- **Discover Elements in the Current Configuration Only.**
- **Exclude Specific Elements from the Search.**

**Limit the Discovery of LANs**

When performing a discovery of LAN/WAN devices that have an uncertified SNMP agent installed, you can limit the discover to LAN interfaces that support basic MIB2 statistics such as In/Out/Total packets. eHealth generates a basic element which allows for reporting of availability and basic packet count information.

**To limit the discovery of LANs**

1. **Access the OneClickEH Console** as a web user who has permission to perform discoveries, and then log in to your eHealth system.
   
   The eHealth Status Summary window appears.

2. **Create a Discover Policy:**
   
   a. In the left pane, select Tasks and Information, Resource Discovery, Policies.
      
      The Create Discover Policy window appears.
   
   a. Select LAN/WAN from the Technology list.
   
   b. Select the Find MIB2 LANs option.
   
   c. Click OK.
      
      eHealth saves the policy to the database.

3. **Run an interactive discover:**
   
   a. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
      
      The Discover window appears.
   
   b. Specify IP addresses (in v4 or v6 format), and then select the discover parameters to include.
   
   c. Click Discover.
      
      The Discover window appears. eHealth generates a basic element which allows for reporting of availability and basic packet count information.

**Important!** To collect vendor-specific interface information when discovering certified devices, do not use the Find MIB2 LANs option.
Use a DCI Rule to Include or Exclude Elements

By creating a Database Configuration Information (DCI) rule, you can include or exclude elements based on certain system element attributes such as element name substring, element type (such as Ethernet), index range, and enterprise ID. If you specify that rule during discovery, discover filters its search based on that rule. For specific instructions on creating DCI rules, see the eHealth Data Integration Guide.

To filter discovered system elements by specifying a DCI rule

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth system.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, Resource Discovery, DCI Rules.
4. In the Create DCI Rule window, specify or change any of the following conditions for the rule:
   - For the Name field, use regular expression syntax to filter based on element names. For example, to filter all element names that match -PVC-, specify the following:
     .*-PVC-.*
   - For the Index field, use commas and hyphens to specify a range. For example: 1,2,5-8
   - For the Enterprise ID field, specify one or more enterprise IDs using a device-specific value. For more information, consult the documentation associated with the device.
      The conditions for the rule change to include or exclude elements based on the specified criteria.
5. Click OK.
   eHealth saves the rule, and closes the Create DCI Rule window.
6. (Optional) Create more rules by repeating steps 3 through 5.
7. Create a Discover Policy based on the System technology type and one or more user-defined DCI rules. All of your rules should appear in the Create New Policy window. For detailed instructions on creating policies, see To create a Discover Policy on page 39.
8. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
    The Discover window appears.
9. Select the Options tab.
10. Using v4 or v6 format, specify the IP addresses for which eHealth should search. Follow the guidelines provided on page 41.
11. Select the Discover Policy name and specify a community string.
12. Click Discover to start the discover process.
    eHealth applies the rule to the discover and includes or excludes elements from the search based on the criteria specified in the rule.
Search for Specific IP Addresses

If you want eHealth to discover a specific set of elements, you can create an ASCII file of IP addresses (in v4 or v6 format) and community strings. For example, to discover an element with an IP address of 10.20.30.40 on SNMP port 6200, a read-write community string of acmeRw, and a read-only community string of acmeRd, enter the following:

```
10.20.30.40 acmeRw/acmeRd 6200
```

To use a file to discover elements

1. Create a file that contains the IP addresses and community strings of the elements that you want to discover, and save the file to local directory on your eHealth system. Use the following format:

   ```
   IP_Address community_string port
   ```

   eHealth saves the file.

   **Important!** The discover process interprets any entry in the format `aa.bb.cc.dd` as an IP address. Do not use ranges or patterns. eHealth does not recognize an IP address range or pattern in a file.

2. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth system.

   The eHealth Status Summary window appears.

3. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.

   The Discover window appears.

4. Select the Options tab.

5. Select IP Address List from File and specify the full pathname of the ASCII file that you created. You can also browse to select the file.

   The file appears in the IP List From File field.

6. If you included community strings in the file, select Use Community Strings from File.

7. Select a policy from the list. If you do not have any policies available, Create a Discover Policy.

   **Important!** The discover process will locate elements with those community strings only. Discover bases its search on the community strings specified in any files that you use, including IP exclusion files. If you do not specify community strings in the file, eHealth uses the ones that you specify in the Discover window.

8. If you want eHealth to update the IP address of the element and the community string, respectively, when you perform a discovery in the future, modify the Discover Policy to set the discover parameters Update IP Addresses and Update Community String to yes.

9. Click Discover.

   The Discovering window appears. Discover searches for resources located at the IP addresses listed in the file only.
Rediscovery

Discover Elements in the Current Configuration Only

You can reduce the length of the discover process by focusing your discover on the elements that exist in your current configuration only. If you tailor your discovery in this way, discover does not identify new elements and give you the opportunity to add them to your configuration. It simply searches for the elements that currently exist and updates your database with any changes.

**To discover elements in the current configuration only**

1. **Access the OneClickEH Console** as a web user who has permission to perform discoveries, and then log in to your eHealth system. The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover. The Discover window appears.
3. Select the Options tab.
4. (Optional) Select a technology.
   - **Note:** If you rediscover a very large configuration (of 100,000 elements or more), it can take many hours. As a best practice, limit the scope or your rediscoveries by specifying a technology for each one.
5. Select Current Configuration.
6. Click Discover. The Discover window appears. eHealth searches for any elements in your configuration that have changed.

Exclude Specific Elements from the Search

If you know the IP addresses of resources that you do not want to monitor, add the addresses to an IP exclusion file. If you specify that file when you perform your discovery, eHealth ignores the addresses. You could also use an existing log file to exclude certain addresses. For example, if you specify the discoverResults.log file that resides in the log directory of your eHealth installation, eHealth will ignore any IP addresses specified in the previous discover process.

**Important!** When you enable the Use Community Strings from File option, always specify matching community strings in IP exclusion files so that Discover excludes the IP addresses properly.

**To exclude elements from a discovery**

1. Create a text file that contains a list of individual IP addresses (in v4 or v6 format), and save the file to a local directory on your eHealth system.
   - **Important!** The discover process interprets any entry in the format `aa.bb.cc.dd` as an IP address. eHealth does not recognize an IP address range or pattern in a file.
2. **Access the OneClickEH Console** as a web user who has permission to perform discoveries, and then log in to your eHealth system.
   
The eHealth Status Summary window appears.

3. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
   
The Discover window appears.

4. Select the Options tab.

5. Select IP Address Exclusion File and specify the full pathname of the ASCII file that you created, or browse and select a file.
   
The file appears in the adjacent field.

6. Click Discover.
   
The Discovering dialog appears. Discover excludes from its search all IP addresses listed in the file.

---

**How to Configure eHealth to Discover SNMPv3 Elements**

To monitor SNMPv3 devices in your infrastructure, you need to configure eHealth to discover and poll these types of elements using the SNMPv3 protocol. The discover process may take longer than a typical discovery due to the extra security validation involved with SNMPv3.

**To configure eHealth to discover SNMPv3 devices, do the following:**

1. Install and configure the SNMP Security Pack™ software (from SNMP Research International) on your eHealth system. For more information, see the *SNMP Security Pack Quick Start Guide*.
   
   **Note:** During the installation setup, you must identify the network management software that you want to use with the service pack.

2. Set the SNMP v3 - Proxy Address to specify the IP address and port number of the BRASS™ server installed as part of the SNMP Security Pack software (Default: 127.0.0.1:4747). For instructions, see the *eHealth Commands and Environment Variables Reference Guide*.

3. Import SNMPv3 key configuration information for each of the devices that you want to discover using SNMPv3 protocols. For instructions, see the *eHealth Data Integration Guide*.

4. Perform a discovery. The first time that you discover an element using the SNMPv3 protocol, the discover process may time out due to the extra security validation involved with SNMPv3. If the process times out, and you receive a NoResponse error message, modify the Discover Policy to increase the setting of the Timeout parameter. For instructions, see Run an Interactive Discover on page 41.
How to Increase the Number of Devices That eHealth Discovers

During discover, eHealth attempts to discover a maximum of four devices at a time. If you have a high-performance workstation, you can improve discover performance by modifying the Max Finder Processes Discover Policy parameter to increase the number of devices that eHealth discovers at a time.

**Important!** Increasing the discover limit can impact system performance because eHealth consumes too much CPU during discovery.

For complete instructions, see Run an Interactive Discover on page 41.

How to Automatically Save to Groups during a Discovery

After you discover elements, you can use the OneClick for eHealth console to organize them into related groups. To expedite the process, you can automatically add elements to existing groups as you discover the elements. If you specify multiple groups, eHealth places all elements in each of the groups.

**Important!** If you used the Options dialog to specify an element filter, be aware that eHealth adds the discovered elements to the specified groups. If you specify a different group name in which to save the discovered elements, you will not be able to view the elements until you change the element filter.

**To automatically save to groups during discovery**

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth system.
2. Create a Discover Policy, and specify the name of one or more existing groups in the Groups field.
3. Run an Interactive Discover.
   
eHealth searches for the resources located at the specified IP addresses and adds all of the elements that it finds to the specified groups.

Community Strings

The community string is an SNMP password that administrators assign to devices to control read and write access to data that is stored in the MIB. By default, eHealth performs a discovery based on the public community string. For most devices, eHealth needs to know only the community string for read access (a read-only community string). However, some device agents use several strings to protect information in the MIB. Some elements, such as service response elements, require read-write community strings to allow eHealth to monitor them.
When you specify multiple community strings, eHealth runs a separate discover process for each one. The first discover process finds elements at SNMP agents that use the first community string. The second discover process finds elements at SNMP agents that use the second community string, and so on. To reduce this overhead, you can filter your discovery by using a file that lists IP addresses and their associated community strings. For instructions, see Search for Specific IP Addresses on page 50.

When you specify a community string, follow these guidelines:

- Include a maximum of 64 single-byte or 32 double-byte characters including the letters A through Z and a through z, commas, backslashes, dollar signs ($), and the numbers 0 through 9.
- Do not include spaces.
- If you include a comma in a community string through a Discover user interface on a UNIX or Windows system, you must supply a backslash character as an escape character. Do not include the escape character when using commas in a community string at the command line.
- If Technical Support advises you to run the discover process through the CLI, and you choose to include a backslash in a community string, follow these guidelines:
  - On a UNIX system, supply an additional backslash as an escape character. On a Windows system, do not supply the extra backslash escape character.
  - If you include a backslash in a community string through the Discover user interface on a UNIX or Windows system, do not supply the extra backslash escape character.
- Specify the correct letter casing. The community string is case-sensitive.
- If you specify more than one string, separate each string with a comma, but do not insert a space between the comma and the next string.
- Specify both read-write and read-only community strings by entering the read-write string, a slash (/), and then the read-only string, as follows:

  `acmeRw/acmeRd`

**Enable eHealth to Find System Processes**

If you have installed a system agent, you can define process sets for the applications that are running on your systems. After discover finds systems, eHealth polls the agent to obtain statistics on the discovered processes and creates elements for them in your database. After eHealth completes the discover process and successfully polls the process set data, you can generate reports to determine the impact of a process set on certain system variables, such as CPU utilization.
To enable eHealth to discover system processes

1. **Access the OneClickEH Console** as a web user who has permission to perform discoveries, and then log in to your eHealth system.

2. Create a process set:
   a. In the left pane, select Tasks and Information, Resource Discovery, Process Sets, and then right-click and select New Process Set. The Create Process Set window appears.
   b. Specify the name of the process set.
   c. (Optional) Define the version of the application that you want to monitor.

      **Note:** The version value appears, but eHealth does not validate your entry. This is a descriptive field.

   d. Click OK.

      The new process set should appear in the left pane under Process Sets.

   e. Right-click the process set name and select New Process.

      The Create Process window appears.

   f. Specify the name of a process as it appears in the system’s process list. Use the actual string for which the discover process searches. To view this information from an AdvantEDGE View Process Information query, see the eHealth Help.

   g. Do one of the following:

      - Accept Full Name next to Match (the default) to enable eHealth to create a process set when it detects a running process whose name matches the text that you specified in the Process Name field.
      - Select Root Name to enable eHealth to create a process element when it detects a running process whose root name contains the text that you specified in the Process Name field (excluding arguments).

   h. (Optional) Do any of the following:

      - If you have multiple processes that have the same name and use unique fixed arguments when they are run simultaneously, specify a string in the Arguments field to uniquely identify this process. For example, if you were creating a process set to monitor your eHealth system, you could create a process named nhiPoller and specify the -live argument in its definition to instruct your system to monitor the Live Trend poller process.
      - If the process is a unique and persistent process for the application, select Key Process to enable eHealth to create elements for all processes in the process set when it discovers this process.
      - If you do not want eHealth to include a process when determining a process set’s availability, deselect Mandatory Process.

   i. (Optional) Exclude these processes from the eHealth calculation for total CPU utilization.

   j. Specify the operating system on which the process can run, and click OK.

      The Create Process window closes.
3. Create a Discover Policy based on the System technology type, and select Find Processes. For detailed instructions on creating policies, see To create a Discover Policy on page 39.

4. Run an interactive discover based on that policy. For detailed instructions, see Run an Interactive Discover on page 41.

   eHealth finds those processes during the discover process and the systems. eHealth then polls the agent to obtain statistics on the discovered processes and creates elements for them in your database.

Maintain Data Continuity for Rebooted Systems

If a device experiences a failure, the SNMP index values may change which will prevent eHealth from being able to poll it successfully. If the system that reboots does not have a discover key or a unique MAC address, you must rediscover it so that eHealth continues to collect data for it.

If a reboot occurs on a few systems, you can change the SNMP index in the database manually. If an event occurs on several systems, you can automate the process by discovering with a seed file.

To maintain data continuity for rebooted systems

1. Enter the following in a command prompt window to identify all elements that have rebooted:

   ```
   nhListElements -rebooted -outFile file.txt
   ```

   eHealth searches the messages.stats.log file for rebooted devices and generates a seed file containing a list of their IP addresses and community strings.

2. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage discoveries.

3. In the left pane, select Tasks and Information, Resource Discovery, and Interactive Discover.

4. In the Discover window, do the following:
   b. In the IP Address List from File field, specify the name of the seedfile that the command generated.
   c. Click Discover.

   The Discover window appears. eHealth locates the devices that have been rebooted and updates the SNMP index values to enable the poller to collect data on the devices.

   If you want to automate this process, contact CA Technology Services for assistance in formulating Live Health Notifier rules that can work with the command line interface to enable the rediscovery of devices after they reboot.
Scheduled Discover Job

A scheduled discover job is a system process that automatically maintains the element definitions in your database so that they continue to respond to eHealth polls. When a scheduled discover job runs, eHealth discovers elements at the specified IP addresses and creates the Discover.jobId.log file, which contains a list of the results for each IP address discovered. eHealth saves this file in the $eHealth/log directory.

How eHealth Saves the Results of a Scheduled Discover Job

During the discover process, eHealth reports any previously discovered elements in the specific IP range that were not found during the current discover process because the device was powered off, removed from the infrastructure, or not the same type as those that you are discovering. After a scheduled discover job finishes, it saves the changes automatically; however, it is more conservative in making changes to the database than the interactive discover process.

When you save the results of a scheduled discover job, eHealth does the following:

- Updates existing elements in the database using the current discover configuration for ports and element naming conventions.
- Ignores duplicate elements.
- Adds new elements.
- Adds new keyed component elements to existing devices in the database.
- Does not make unresolved updates to the database (that is, it does not match the element based on less reliable attributes such as MIB index and MTF if it cannot match on discover key or physical address).

**Important!** If you do not want the scheduled discover job to automatically save the changes, you can modify the job.

How to Run Effective Scheduled Discoveries

After you run an interactive discovery once, create a scheduled discover job to automatically maintain the element definitions in your database so that they continue to respond to eHealth polls.

To run an effective discover scheduled job, follow these best practices:

- Always review the discover log of a scheduled discover job to identify unresolved changes, and then run an interactive discover process or modify the element information to resolve the changes.
- Do not modify, add, or delete elements while a scheduled discover job is running. If you make changes, you must cancel the changes after the discover has finished.
**Scheduled Discover Job**

**Important!** Scheduled discover jobs do not update in an open element window. To view changes that were made by a scheduled discover job, you must close and reopen the window.

- Disable elements or add them to an exclusion file to prevent eHealth from rediscovering them.

**Set Up a Scheduled Discover Job**

By default, eHealth automatically saves the results of a scheduled discover job in the eHealth database and updates the database with any changes that have occurred. When you set up a scheduled discover job, you can prevent the discover process from saving the changes, and you can also specify the e-mail address of a user who needs to review the discover log file following the completion of the job.

**To schedule a discover process**

1. **Access the OneClickEH Console** and log in to the eHealth system as a web user who has permission to manage discoveries.
2. **Create a Discover Policy**.
3. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
4. In the Discover window, select the Options tab.
5. Specify the IP addresses (using v4 or v6 format), the policy name, and the community string, and then select the Schedule tab.
6. In the schedule window, specify the days and the time, and specify an e-mail address of any user who would like to review the log file.
7. Click Schedule Job.

**Modify Interface Elements to Record Detail Data**

To run LAN/WAN reports on router interface elements, you must enable eHealth to save detailed performance data on those elements when you discover them using the Router/Switch Discovery technology.

**To record detail data for interface elements**

1. **Access the OneClickEH Console** as a web user who has permission to manage elements, and then log in to your eHealth system.
2. Select Managed Resources, Elements in the tree.
   The Elements window appears.
3. Double-click the router interface elements on which you want to report.
   The Edit Element window appears.
4. Select the Polling tab, select Yes from the Record Detail Data list, and click OK.
eHealth now reports on the router interface elements when you generate reports.

**Important!** If you deselect Record Detail Data and perform a rediscovery, discover checks the setting of the option for each interface on the router. If only a few of your interfaces (or none) are configured to record detail data, OneClickEH discovers the router/switch elements using only the Router/Switch technology, updates them, and adds any new elements. You must enable the Record Detail Data option for all interfaces manually using the Edit Element window. If all interfaces on the router/switch have the option enabled, OneClickEH rediscovers the interfaces using both Router/Switch and LAN/WAN technologies. If it finds new interfaces, it adds them and enables the option by default. If you want to disable the option, you must do so manually.

### How to Improve Your Discoveries

To keep the database up-to-date with your infrastructure, you should take steps to prevent unresolved elements by helping the discover process identify changes that have occurred to the devices that you are monitoring. Following a discovery, you should make it a practice to reconcile unresolved elements before you attempt to rediscover them.

To improve your discoveries, follow these best practices:

- Use the same IP address discover strategy each time, and always keep your IP address list files and exclusion files up-to-date.
- Prevent discover from interpreting multiple changes to a device as a new element. Make one change and then rediscover, or update the database with a few changes before you discover.
- Specify correct community strings.
- Organize your elements as you discover them. Use Groups discover feature to save your elements to existing groups automatically.
- Enable discover to identify devices as unique devices based on the matching algorithm. Use unique sysName and uniqueDeviceId values for each device.
- Enable discover to differentiate among multiple device interfaces. If you used the same ifDescr MIB variable for more than one device, modify element properties to eliminate any duplication.
- When you upgrade the operating system or SNMP agent software, discover before and after upgrading.
- If you remove or move a component (or replace it with entirely different hardware), delete or retire the old element.
Chapter 4: Maintaining Your Element Configuration

This chapter contains the following sections:

- Elements
- The eHealth Poller
- Poller License Consumption
- Common Polling Problems
- Element Properties
- Element Removal
- Element Creation

Elements

After eHealth discovers a resource, it adds it as an element—its representation of your business resource—to the database. eHealth monitors two types of elements within an infrastructure: *statistics* elements, which are devices and interfaces within the network; and *conversation* elements, which monitor traffic flow among nodes and applications using the network. Using the OneClick for eHealth console, you can view and manage all elements that eHealth is monitoring.

View Your Element Configuration

To view all elements that you are monitoring and their associated configuration information, you can use the OneClickEH console.

To view your element configuration

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements.
By default, OneClickEH immediately shows all of your elements in the console. If you specify matching criteria in the Filter table by field at the top of the console screen, it filters the list as you type.

**Note:** If you have a very large configuration, OneClickEH can require several minutes to show the entire list.

3. (Optional) Select Tools, Options, Advanced at the top of the console to customize the element display. Do either or both of the following:
   - Prevent OneClickEH from displaying the entire element configuration. Deselect Show all elements or all nodes immediately.
   - Control the number of elements or nodes that appear in the element table. Specify a value in the Number of elements or nodes shown on each page field.
   - Click OK.

4. Select Managed Resources, Elements in the OneClickEH tree. The Elements page appears, but does not display any elements.

5. Filter your element search based on a specific name, alias, or IP address.
   - If you select Alias from the list, you can specify a portion of the element’s alias name using wildcards (for example, *testSystems*).
   - If you select Name from the list, you can specify a portion of the element’s name using wildcards (for example, *boston*).
   - You can also search for one or more IP address octets using wildcards. All sample formats shown in the following table are valid:

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>111.*</td>
</tr>
<tr>
<td></td>
<td>*.11</td>
</tr>
<tr>
<td></td>
<td>111.11.*.50-100</td>
</tr>
<tr>
<td></td>
<td>111.<em>.11.</em></td>
</tr>
<tr>
<td></td>
<td>111.11.23-30.*</td>
</tr>
<tr>
<td></td>
<td>111.11.11.*-30</td>
</tr>
<tr>
<td>List</td>
<td>111.11.13,15,17.*</td>
</tr>
<tr>
<td></td>
<td>20,27,32.11.*.11</td>
</tr>
</tbody>
</table>

**Important!** You can use the * symbol as a wildcard to search for all numbers within the range of 0-250, but you cannot use the wildcard to search for a single digit.

6. Click Go to complete the operation.
   The tables refreshes and displays only the elements that match the criteria. If necessary, sort, move, reorder, or resize the columns to find elements of particular interest to you.

7. (Optional) Filter the content of the table further by entering text in the Filter table by field and pressing Enter.
   eHealth filters the display based on the text string.

**Note:** You can prevent eHealth from filtering the element list until after you finish specifying all of your matching criteria by selecting Tool, Options, Advanced from the menu at the top of the console, and deselecting Filter element tables as you specify the filtering criteria.
View Elements in the eHealth Console

The eHealth console sorts all elements in the Poller Configuration dialog alphabetically by name. Using various options, you can reorder and filter the list to show specific elements, and manage all of your element types. If you enable the global setting in the Options dialog to display alias names, the dialog shows aliases in the list in place of the actual element names.

To search for a specific element in the eHealth console

1. Log in to the eHealth console as an administrator. The eHealth console appears.
3. Do one of the following:
   - Enter a string in the Search for Name field with a wildcard such as an asterisk (*) to match two or more characters or use a question mark (?) to match any single character. The filter displays the elements that match the specified characters
   - Enter a string without any wildcards. The filter displays the elements that contain that string anywhere in the name.
   - Leave the Search for Name field empty. The filter displays all elements.

How to Save Element Information

To manage element information, you can save it by outputting it to a file. The information can be useful for inventory checking and for reviewing the elements that you are monitoring. For example, you could use it to devise a list of alias names.

To save element data, use one of these methods:

- In the Elements window of OneClickEH, right-click, select Export All, and then save all data to a .csv file. You can also save selected entries to a file.
- In the Poller Configuration dialog of the eHealth console, use the Save List To File option to save all configuration data displayed in the dialog to an ASCII file named poller.cfg.log in the /eHealth/log directory. If the file already exists, eHealth overwrites it with the new information.
- Run the nhListElements command to output a list of element names that exist in your database.
The eHealth Poller

The eHealth poller is the software tool that automatically collects data for any element that has been saved in the eHealth database through the process of discovery. The database defines the information for each element such as the name, a polling rate (the frequency with which eHealth polls the element), and the agent type (the type of element that eHealth discovered).

Polling

The process that the eHealth software uses to collect performance and availability statistics on the resources that it is monitoring.

Polling Interval

The rate at which eHealth collects statistics data and conversation data.

Conversation Poll Rate

The conversation poll rate is the speed at which eHealth collects data on the probes and other devices that you are using in your network to collect traffic data. The default poll rate for conversation data (which applies to data collected by Traffic Accountant) is 30 minutes, but you can set it to 15, 45, or 60 minutes. The polling interval is longer than that for statistics data because eHealth polls each Traffic Accountant probe to collect data on every conversation that the probe detected, which can result in a tremendous amount of data being collected at each poll.

Statistics Poll Rate

The speed at which eHealth polls statistics elements.

Normal Polling Rate

By default, eHealth assigns the Normal polling rate to newly discovered statistics elements. It polls elements every 5 minutes and saves the data to the database during the poll. This is the rate that you should typically use to collect data from statistics elements.

Slow Polling Rate

eHealth polls elements every 30 minutes and saves the data in the database during the poll. You can change the default interval to 10, 15 or 60 minutes. The Slow polling rate allows you to poll elements that you want to poll less frequently because you do not expect their utilization rates to change.

Fast Polling Rate

eHealth aggregates the data from five 1-minute polls into one 5-minute average sample before saving it to the database. This process maintains consistent data samples. You can change the default interval to 30 seconds, 2.5 minutes, or 5 minutes.

Fast Store Polling Rate

eHealth collects data at the Fast rate and stores the 1-minute samples in the database without aggregating them.
Set the Poll Rate and Interval for All Statistics Elements

The eHealth poller runs continuously to regularly collect data from elements. To troubleshoot problems, you can use the Poller Controls window in the OneClick for eHealth console to stop the poller for all elements that you are monitoring. When you turn off polling, you are turning off the statistics, import, and conversation pollers, so eHealth does not poll any elements and reports show a gap during that time period.

You can also use the Poller Controls window to specify the times and rates at which the poller runs. For example, if you do not want to collect data all day or every day of the week, you can configure the poller to run only during certain hours of the day and you can change the rate at which it polls elements.

To set the poll rate and interval for all statistics elements

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage elements.
2. In the left pane, select Setup, Poller Controls.
   The Poller Controls window appears.
3. Do any or all of the following and click OK:
   - Turn the poller on or off.
   - Change the poll interval for all elements to control the amount of data that you collect.
   - Change the statistics polling schedule.
   - Change the poll rate.

The Poller Controls window closes, saves the changes, and begins polling at the specified interval in accordance with the modified schedule.

Set the Poll Rate for Individual Statistics Elements

For individual elements, you can use the OneClick for eHealth console to set the poll rate to Normal, Slow, Fast, or Fast Store. To resolve a polling problem, OneClickEH allows you to quickly change any element to the Fast rate by right-clicking on it. Typically, you should only use the Fast rate to collect data more frequently from high-speed devices that do not support 64-bit counters, such as FDDI or ATM interfaces. High-speed element agents collect a significant amount of data during a Normal (five-minute) polling period. If a high-speed interface indicates significantly less volume than you expect, or it generates a large delta error, polling it at the Fast rate can prevent eHealth from missing data. The Fast rate is also effective for collecting data from modems or ISDN connections that have short-duration connections.

- When it polls at the Fast rate, eHealth aggregates the data from five one-minute polls into one five-minute average sample before saving it to the database.
- When it polls at the Fast Store rate, eHealth saves the one-minute samples and does not aggregate them.
Therefore, when you use the Fast or Fast Store rate, your system performance requirements increase. Depending on the size of your eHealth system, if you poll too many elements at the Fast rate, the poll might not finish before the next Fast poll is scheduled to begin. To determine the equivalent polling load, multiply the number of Fast-polled elements by the ratio of Normal poll rate to Fast poll rate, and add that number to your total number of elements. For example, if you have 5000 elements, and 200 are polled at the Fast rate, the poller is actually performing \(4800 + (200 \times 5) = 5800\) polls during a Normal 5-minute polling interval.

**To set the poll rate for individual statistics elements**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. Select Managed Resources, Elements in the tree. The Elements window appears.
3. Double-click the element name in the element table. The Edit Element window appears.
4. Select the Polling tab, select a polling rate, and click OK. eHealth resets the polling rate for that element.

**Set the Poll Rate for All Conversation Elements**

Probe memory can vary and determines the amount of conversation data that eHealth collects from the probe. Use a polling interval that allows you to retrieve data from the probe before it resets counters or drops data. The number of elements in your database and the amount of disk space available for the database might require you to use a polling interval that is longer than the default.

**To set the poll rate for all conversation elements**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage elements.
2. Select Setup, Poller Controls. The Poller Controls window appears.
3. Do any or all of the following and click OK:
   - Turn the poller on or off.
   - Change the conversations poll rate.
   - Change the polling schedule.

The Poller Controls dialog closes, saves the changes, and begins polling conversation elements at the specified rate in accordance with the modified schedule.
How to Maintain the eHealth Element Configuration

Managing element data that eHealth collects on your resources is a critical administration task. While discover can keep the majority of your element information up-to-date automatically, the discover process works most effectively when you maintain your configuration as your infrastructure changes over time. Complex devices such as large-scale routers or systems can constantly change with the addition or removal of components. These types of complex devices could experience multiple changes at one time, so you may need to manually update the database to reflect these changes.

If you do not actively manage and maintain your element information, errors will occur during the discover process and eHealth will not be able to successfully collect data on your resources.

As the following changes occur within your infrastructure, your database can become out-of-date quickly:

- Adding or removing devices from your infrastructure.
- Changing MIB attributes or the agent at a device.
- Adding or removing interface cards, disks, CPUs, or partitions for devices.
- Upgrading or restarting applications, operating systems, or SNMP agents at devices.
- Changing interface bandwidth and speed.
- Assigning new IP addresses to interfaces.

To maintain your element configuration and data continuity, do the following:

1. Review your discover logs carefully, verify the changes, and update the element information that discover was unable to change.
2. Retire or delete elements that you no longer want to monitor and those that are no longer part of the infrastructure.
3. Tailor rediscoveries by using a filtering method to find only the elements that you want to monitor.
4. Identify and resolve polling problems so that eHealth can continue to collect data. Monitor polling to identify errors, and correct the problems as soon as possible.
5. Add new resources by manually adding elements to the database that discover is unable to find.
6. Facilitate reporting and management by organizing related elements into groups.
Poller License Consumption

You can discover any number of elements; however, eHealth will only poll elements that have a poller license. eHealth uses poller licenses to control the number of elements that you can poll. Although most elements only consume one license, some share a license; therefore, it is important to track the number of licenses that eHealth requires for all of the elements in your database.

How to Manage Poller License Consumption

You can only poll elements for which you have available poller licenses. In some cases, two elements may share a license. To identify those elements that are the primary consumers of a license, review the Poller License Status field in the OneClickEH Elements window. If multiple licenses have the same License ID, they share a license. You can manage your poller license consumption from the OneClickEH Status Summary window that appears immediately after you log in to your eHealth system.

Important! For instructions on purchasing additional licenses, see the Technical Support web site.

To manage poller license consumption, follow these steps:

1. Review the OneClick for eHealth Status Summary window to identify the following:
   - number of poller licenses that are available for use
   - total number of licenses that you have
   - total number that you need to poll all of your elements
2. Identify any elements that you do not need to monitor, and then free the licenses that they are consuming by turning off polling for those elements or deleting them.
   Note: When you turn off polling for an element, it remains in the database, but it does not require a license because eHealth is no longer collecting data for it. For detailed instructions, see Redistribute Polling Licenses on page 68.
3. Use the nhListElementLicenses command to identify the primary consumers of a license and those elements that share a license with another element, do not need a license, or are not consuming a license.
4. Delete or disable all primary elements that share the same license to free those licenses for use.

Redistribute Polling Licenses

If you do not need to monitor all of your elements, you can free some licenses by turning off polling for them or deleting them. When you turn off polling for an element, it remains in the database, but it does not require a license because eHealth is no longer collecting data for it.
To free a license for use by another element

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane of the console, select Managed Resources, Elements. The right pane refreshes and displays all elements in your database.
3. Right-click the element in the OneClickEH table and select Disable Polling. eHealth stops polling that element.
4. Double-click the element that needs the license. The Edit Element window appears.
5. Select the Polling tab, select Yes from the Polling Enabled list, and click OK. eHealth automatically assigns the free license to that element and begins polling it.

Common Polling Problems

Typically, polling problems can result from temporary or prolonged network delays or connection problems, element index shifts, and traffic congestion. You can also receive errors if you are polling devices that have not been certified for use with eHealth, polling information is out-of-date, or the polled device does not respond to an eHealth poll within a specified amount of time.

How to Resolve Common Polling Problems

You use the OneClick for eHealth Polling Management interface to identify all elements that have reported polling problems during the last Normal polling period, and the time period for which eHealth has not collected data.

If an element does not respond to ping, but you know that it exists, check the configuration of the element to confirm that it matches the properties that have been saved in the database.

Important! Any changes that you make to statistics or conversation elements take effect during the next poll. The poller does not restart; the changes take effect without interrupting the polling cycle.

Resolve “No Such Name” Polling Error

eHealth generates a "No Such Name" polling error when polling information is out-of-date because the agent does not have a MIB entry at the requested OID.
Common Polling Problems

To resolve a “No Such Name” polling error

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane of the console, select Polling Management, No Such Name. The console displays those elements that have generated that type of error.
3. Select the element, right-click, and select Rediscover.
4. If the SNMP error persists, do the following:
   a. Confirm that the device responds to SNMP V1 “get” commands.
   b. Verify that the device is certified for use with eHealth. Search for the device at http://support.concord.com/devices/html/search.html.
   c. The device may be certified for use with SNMPv2 only. If you are using SNMPv3 by proxy through SNMP Research SNMP Security Pack, confirm that the SNMP security pack is configured correctly.

Resolve “Device Exceeded Allowable Timeouts” Polling Error

When devices with multiple elements such as routers or servers do not respond to SNMP requests, the information that the poller collects is incomplete. In addition, if those elements are consistently unresponsive, the performance of the poller is negatively impacted. To maintain the accuracy of polled data and limit the amount of time that eHealth spends polling one device, eHealth tracks the number of SNMP request timeouts. If it exceeds the value of the NH_SNMP_DEVICE_TIMEOUTS environment variable, it stops polling any elements associated with that device and proceeds to poll the next device.

To resolve a “device exceeded allowable timeouts” polling error

1. Wait one or two more polling cycles to see if the device responds.
2. Change the setting of the NH_SNMPDEVICE_TIMEOUTS environment variable.
3. Change the setting of the NH_SNMP_RETRIES environment variable.
4. If the device does not respond, contact the device owner to determine if the element information is incorrect or the SNMP agent is down.

Resolve “Received Large Delta Error” Polling Error

A counter wrap occurs when one or more MIB variables reaches its maximum value, resets to zero, and begins counting again within one polling cycle. When the delta, which is the difference between the counter values for the last poll and the current poll, reaches or exceeds 50% of its maximum value, eHealth identifies this as a large delta error. It discards the data for that element for that poll because the counter wrap can cause unusual results in reports and performance monitoring.
To resolve a “received large delta error” polling error

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Polling Management, Received Large Delta Error. The console displays those elements that have generated that type of error.
3. Select the specific element that experienced the error.
4. Change the statistics polling rate. Right-click it and select Fast Poll to Resolve Large Deltas.

The poller should poll this element successfully on the next scheduled poll.

Resolve “No Response (to SNMP)” Polling Error

If the polled device does not respond to an eHealth poll within a specified amount of time, eHealth generates an error and does not collect any data for that element for that poll interval.

To resolve a “No Response (to SNMP)” polling error

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Polling Management, No Response (to SNMP). The console displays those elements that have generated that type of error.
3. Select the specific element that experienced the error, and do one of the following:
   - If the agent is running, the problem may be due to temporary network delays. Wait a few poll cycles to see if the error persists.
   - If the element has never responded to SNMP requests or is intermittent, increase the time that eHealth waits for an SNMP response. Modify the setting of the NH_SNMP_TIMEOUT environment variable. To prevent wasteful increases in the overall poll cycle time, increment the value by one million and then wait to observe the impact.
   - Rediscover the element and wait for the next scheduled poll.

The poller should poll this element successfully on the next scheduled poll.

Important! If polling is not successful, see the Poller Tuning Guide which is available on the Support web site.

Resolve “Received an SNMP Error” Polling Error

The eHealth poller generates a “Received an SNMP Error” polling error when polling information is out-of-date because the element had an index shift or the device has not been certified by CA.
To resolve a “Received an SNMP Error” polling error

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.

2. In the left pane, select Polling Management, Received an SNMP Error. The console displays those elements that have generated that type of error.

3. Select the specific element that experienced the error, and do one of the following:
   a. Right-click and select Rediscover.
   b. If the SNMP error persists, do the following:
      - Confirm that the device responds to SNMP V1 “get” commands.
      - Verify that the device is certified for use with eHealth. Search for the device at http://support.concord.com/devices/html/search.html.

      Note: The device may be certified for use with SNMPv2 only. If you are using SNMPv3 by proxy through SNMP Research SNMP Security Pack, confirm that the SNMP security pack is configured correctly.

   The poller should poll this element successfully on the next scheduled poll.

Resolve “No Response to Ping” Polling Error

The eHealth poller generates a "No Response to Ping” error when an IP address for an element does not respond to the ping request that eHealth sends to it before it sends an SNMP request. eHealth considers it to be a missed poll and does not collect SNMP data from the device. Ping failures can occur because of network connection problems that either prevent the ping request from reaching the polled device or prevent the ping response from reaching the eHealth system. Ping failures also occur if the device is off. Also, when traffic on the network is congested, routers and switches may discard ping requests in favor of higher-priority traffic.

To resolve a “No Response to Ping” polling error

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.

2. In the left pane, select Polling Management, Received an SNMP Error. The console displays those elements that have generated that type of error.

3. Select the specific element that experienced the error, and do one of the following:
   ■ If the ping failure is local to one or more devices, right-click, select Ping from Server, and do one of the following:
      - If the element does not respond, determine if it is off or has been removed from the network.
      - If the device has been removed from the network, right-click and select Delete or Retire to remove the element.
   ■ If ping errors are occurring for many elements in your configuration and you have confirmed that the cause is not due to temporary network conditions, verify that the address is correct and verify that nothing is blocking ICMP ping packets.
Common Polling Problems

- Change the ping size. The default ping size is 100 bytes, which can cause some problems with certain devices and firewalls. To change the size, you can modify the `NH_POLL_PING_PKTSIZE` environment variable.

- You may have network restrictions that would always prevent a successful ping. In that case, you can disable the ping operation with each poll using the `NH_POLL_PING_DISABLED` environment variable. This will allow eHealth to gather SNMP responses, but calculate reachability based on SNMP responses rather than true device reachability using ping. This will also disable latency for any devices that are configured to collect it.

The poller should poll this element successfully on the next scheduled poll.

**Change Poll Rate**

If an element that is being polled at the Fast rate consistently shows missed polls in the OneClickEH Status Summary window, the element agent might not be able to respond to the SNMP polls during the fast interval. To enable the agent to respond, changing the timeout and retries rates, as well as the `min_request_interval` and `agent_throttle` variables, may solve the problem. For instructions, see the Poller Tuning Guide (available on the Support web site).

**Disable Polling**

When you disable polling for an element, it remains in the database, but eHealth no longer collects data for it. You may want to disable an element to exclude it from reports temporarily or permanently. If you are unable to determine why an element is generating an error after being polled, you can disable polling for it while you try to resolve the error.

**Important!** You cannot disable polling for some elements, such as certain response path elements.

If you disable polling for a router or a system, keep in mind that eHealth also disables polling for all elements that belong to that router or system. However, it continues to poll any router or system interfaces that record detail data unless you specifically disable polling for those interfaces.

**To disable polling for an element**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Elements, Elements.
   The Elements window appears.
3. Scroll to locate the element, right-click, and select Disable Polling.
   A confirmation window appears.
4. Click Yes.
   The window closes, and eHealth stops polling the element.
Change Community String

The community string is used by administrators to grant *read and write access* to various device MIBs. eHealth typically uses a read-only community string to poll devices. If you change the read-write community string or the read-only community string of a device, you must change the community strings that eHealth uses for the element that represents the device. Otherwise, eHealth cannot poll the device. If your web user account has permission to manage community strings, you can change both the read-write and read-only community strings for most elements that you are monitoring.

When specifying community string, follow these guidelines:

- Do not use spaces.
- If you include commas in a community string through the Discover user interface, you must supply a backslash character as an escape character. Do not include the escape character when using commas in a community string at the command line.
- If you include a backslash (\) at the command line on a UNIX system, you must supply an additional backslash as an escape character.
- If you include a backslash (\) at the command line on a Windows system or in the Discover user interface on a UNIX or Windows system, do not supply the extra backslash escape character.
- To change both the read-write and the read-only community strings for an element, double-click it to display the Edit Element window, and then select the General tab. Specify a read-write community string for SNMP Gets and Sets, which includes creating, modifying, or deleting MIB monitoring rows, and automatic licensing, and then specify a read-only community string for SNMP Get requests.

**To quickly change the read-write community string for an element**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Elements, Elements. The Elements window appears.
3. Scroll to locate the element, right-click, and select Modify Read-Write Community.
4. Specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, commas, backslashes, dollar signs ($), and the numbers 0 through 9.
5. Click OK.
Common Polling Problems

Rediscover an Element

If an element generates a "Received an SNMP error," the index may have shifted as a result of a reboot or other configuration change. To resolve the problem, you can right-click the device name in the OneClickEH element table and select Rediscover to try to update the database. Large delta errors may also occur if you have not applied the latest device certification patch. Once you have applied it, you need to rediscover using the same method, or you may just need to fast poll the element.

**Note:** When you rediscover an element to correct polling problems, eHealth runs the discover process based on the saved Discover Policy. If an element does not have a Discover Policy associated to it, you need to edit the element and associate a policy (by selecting the Discovered Information tab in the Edit Element window).

For those devices that may have more than one element, eHealth rediscovers the entire device, not just the one element that is having polling problems. As a best practice, always review the Discover log carefully—before saving the results—to confirm the changes that OneClickEH identifies.

Change Retries and Timeout Rate

If you receive a "No Response (to SNMP)" error for an element that has never responded to SNMP requests or intermittently responds, you can increase the time that eHealth waits for an SNMP response.

By default, eHealth does the following:
- Waits four seconds (4000000 microseconds) before timing out, based on the value of the NH_SNMP_TIMEOUT environment variable.
- Attempts to retry polling three times (based on the NH_SNMP_RETRIES environment variable setting) before skipping the element and recording the poll as a missed poll.

Before performing this procedure, review the guidelines provided in the *Poller Tuning Guide* (available on the Support web site).

**To change the retries and timeout rates for an element**

1. **Access the OneClickEH Console** and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Elements, Elements. The Elements window appears.
3. Scroll to locate the element and double-click it.
4. In the Edit Element window, select Polling.
5. Specify the poll timeout value.

To prevent wasteful increases in the overall poll cycle time, increment the value by 1000000, but by one, and then wait to observe the impact.
6. Specify a value in the Poll Retries field to increase or decrease the number of times that eHealth will attempt to retry polling an element before giving up on the poll.

7. Click OK.

**Element Properties**

The database defines properties for each element including the name, agent type, alias, community string, discovered values, interface speed, parent name, and SNMP index. You can modify most of these element properties by using the OneClick for eHealth console.

**Agent Type**

The agent type specifies the type of element, and thus, the data that eHealth collects from it. The discover process uses the information that is supplied by the agent at the polled device to select an agent type for each element that it creates.

Typically, you can modify the agent type to change system user partitions to system partitions, or to change interfaces to collect MIB2 rather than RMON data:

- eHealth uses different thresholds for system and user partitions because the utilizations and problems are usually very different. System partitions are not expected to change size, and they are often stable even with a high utilization percentage (80% or greater). User partitions often change and grow quickly, and problems can occur if the user partitions are more than 60-70% utilized.

- If interface elements discovered as RMON (Ethernet) agents support MIB2 variables, you can change the agent type to MIB2 (port) to take advantage of the additional information that is collected for MIB2 interfaces.

To change the agent type, you must use the Modify Element dialog in the eHealth console. You cannot use the Edit Element feature of OneClickEH to change this element property.

**Important!** Use care when modifying the agent type of an element; if you select a type that the device cannot support, it could prevent eHealth from polling the element.

**Alias**

An alias is a shorter, more meaningful name that you can assign to an element after you discover it and save it to the database.
Community String

The community string is used by administrators to grant read and write access to various device MIBs. eHealth typically uses a read-only community string to poll devices.

Discovered Information

The Discovered Information values are the values that eHealth obtains from the element agent during a discover. To change the System Description, Location, and Contact values (or to associate a Discover Policy to the element), you can double-click the element and select the Discovered Information tab in the Edit Element window. However, to change any of the other values, you must use the Modify Element dialog in the eHealth console.

Important! As a best practice, only change these values to prevent or resolve duplicate elements that resulted from a discover process, or to update the information to match the associated attributes that have changed at the device level.

Element Name

The element name is the name that eHealth automatically assigns to a resource after it discovers it within your infrastructure. Because discover follows specific naming conventions, the names can be quite long and difficult to identify. eHealth reports often truncate element names that are longer than 30 characters.

Interface Speed

During the first poll, eHealth obtains the speed of LAN elements, and both the incoming and outgoing speeds of full-duplex interface elements as configured at the device. If the device’s configuration does not report the correct speed, you may need to manually modify the element speed so that eHealth can produce meaningful reports. If eHealth sets the speed of Frame Relay devices to 0 because they did not have any speeds configured, you may also need to use OneClickEH to modify it.

You can specify a number, which sets the rate in bits per second, or a number and the letter k (to specify kilobits per second) such as 56 k for 56,000 bits per second. You could also specify m (to specify megabits per second) such as 16 m for 16 Mbits per second (Mbps). eHealth does not accept a speed of zero (0).

Parent

A parent is the top-level element in a hierarchy of elements (such as a router, system, modem pool, or remote access server). For example, a modem pool can have several elements. When you modify the polling status or polling interval of a parent element, eHealth may modify the properties of the child elements to
match. If you attempt to modify the polling status or interval of the child element so that they are no longer compatible with the parent element, eHealth rolls back the change to maintain compatibility with the parent element.

### SNMP Index

The **SNMP index** is a unique identifier for similar elements of a device (for example, all interfaces of a router). A device index can change, or shift, as a result of adding or removing interface cards in a router, upgrading router firmware, changing system elements, or rebooting a device. Index changes can result in an SNMP polling error. If they occur, you can usually rediscover to resolve the problem and update the elements. However, if the changes are too complex for discover to resolve, you may need to manually update them using the OneClick for eHealth console.

Index changes can affect all elements of a device. For example, if you remove an interface card from the first card slot of a router, the indexes for the remaining interface elements could all decrease by one. To enable eHealth to successfully poll these devices, rediscover them.

### How to Update the Properties of an Element

Although discover is able to update elements automatically, you may need to manually update element properties to prevent or resolve discover errors and duplicate elements. Typically, you perform manual updates when the element has changed so drastically that discover cannot match any of its attributes to an existing element, so it considers it a new element. Also, you can perform these changes manually when you need to override the device settings. This might happen when the device configuration is incorrect, but you do not have permission to change the device, or you want to monitor the device in a special way.

**Important!** Any changes that you make to statistics or conversation elements take effect during the next poll. The poller does not need to restart; the changes take effect without interrupting the polling cycle.

To update the properties of an element, do the following:

1. In the OneClickEH console, select the element, right-click, and select Properties.
2. Double-click the element to display the Edit Element window.

When you change element properties, it is important to follow these guidelines:

- Do not modify element properties while a scheduled discover job or a configuration import is running. If the database changes while you are making a change, an error message appears, and you cannot save your changes. You must close the element window, reopen it, and make the changes again.

- If you change the information for an existing device, make the corresponding changes to the information for any component element. For example, if you edit the system name setting for a router, edit the setting for the interfaces and CPUs on that router as well.
Update the SNMP Index

If one or more devices have experienced an index shift, manually change the index for these elements so that eHealth can continue to poll them.

To manually change the SNMP index for elements
1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Double-click the element names in the element table. The Edit Element window appears.
4. Select the Indexes tab and do the following:
   a. Select Mass Modify.
   b. Specify text in one or more of the Index fields.
   c. Click OK.

Specify User Strings to Use as a Filter in OneClickEH

The User String column displays a custom string that you can specify to describe your elements. Typically, you create the string in the Elements section of the DCI file using DCI element configuration input tools. With OneClickEH, you can view, specify, and filter based on those strings.

To add the User String column to your element tables, right-click a column name and select Select Fields. If you have not used DataSync to import your elements, you can specify a user-defined string to use as a filter in OneClickEH. You can also modify or append to any string that you have already defined.

To define a userString value in OneClickEH tables
1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Double-click the element name in the element table. The Edit Element window appears.
4. Select the General tab, specify text in the User String text box or append additional text to the existing string, and click OK.
   OneClickEH saves the change and closes the Edit Element window.
5. Add the column to your element tables by doing the following:
   a. Right-click a column name in the OneClickEH console and select Select Fields.
      The Select Fields dialog appears.
b. Scroll through the Available Fields list to find User String, and double-click it.

The field name appears in the list.

c. Use the arrow to reorder the name in the list and click OK.

The Select Fields dialog closes and the User String field appears in the element table.

**Rename an Element**

When you perform a discovery, eHealth automatically assigns a name to each element that it creates. eHealth reports often truncate element names that are longer than 30 characters. In other cases, the names are not very meaningful, so it is difficult for users to quickly identify the elements. Once you have saved elements in the database, you can make the names more intuitive by renaming them to be more meaningful to administrators or report consumers.

**To rename an element**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.

2. In the left pane, select Managed Resources, Elements.

   The Elements window appears.

3. Double-click the element name in the element table.

   The Edit Element window appears.

4. Select the General tab and specify text in the Element Name field. 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:** Do not specify a name that exceeds 64 bytes or is composed entirely of numerical characters. Do not duplicate another element name in your database. Element names must be unique.

5. Click OK.

   OneClickEH saves the change and closes the Edit Element window.

**To change an element substring in multiple elements**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.

2. In the left pane, select Managed Resources, Elements.

   The Elements window appears.

3. Double-click the names in the OneClickEH table.

   The Edit Element window appears.

4. Select the General tab, specify the element substring by following the character limitations for element names.

5. Click OK.

   OneClickEH saves the change and closes the Edit Element window.
Define an Alias for an Element

If an element name is very long or not very intuitive, you can assign an alias name to the element to make it easier to identify. For example, you might want to change the name of one or more interfaces to indicate the names of the cities to which the interfaces connect or to show that the interfaces are leased lines.

To define an alias for an element

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Double-click the element name in the element table. The Edit Element window appears.
4. Select the General tab and specify text in the Element Alias field. Alias names do not have to be unique.
   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: Do not specify a name that exceeds 64 bytes or is composed entirely of numerical characters.
5. Click OK. OneClickEH saves the change, updates the element, and closes the Edit Element window.

To change or assign an alias substring for multiple elements

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Double-click the names in the OneClickEH table. The Edit Elements window appears.
4. Select the General tab and do the following:
   a. Select Mass Modify.
   b. Specify the alias substring by following the character limitations for element names.
   c. Click OK. OneClickEH saves the change and closes the Edit Element window.
Modify a Parent Setting

If you move an element from one device to another, you should modify its parent setting. For example, if the element is on a router or system, change the parent name of that router or system element. When you modify a parent element, eHealth modifies certain properties of the child elements to match. If you attempt to modify properties of the child element that cause inconsistencies with the parent element, eHealth rolls back the change to maintain consistency with the parent element.

To modify a parent setting

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Poller Configuration.
   The Poller Configuration dialog appears.
3. Select the elements to which you want to assign a parent name and click Modify.
   The Modify Elements dialog appears.
4. In the Change Parent To field, specify the parent name and click OK.
   eHealth saves the change and updates the element.

Exclude an Element from Live Exceptions Monitoring

Live Exceptions monitors eHealth elements to detect conditions defined by alarm rules. When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list; however, you can exclude an element from Live Exceptions monitoring by manually modifying the element. You can also select the time zone within which Live Exceptions should monitor the element.

To exclude an element from Live Exceptions monitoring

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage elements.
2. In the left pane, select Managed Resources, Elements.
   The Elements window appears.
3. Double-click the name in the OneClickEH table.
   The Edit Element window appears.
4. Select the General tab and do the following:
   a. Select Yes from the Monitor in Live Exceptions list.
      Important! If you have not installed a license for Live Exceptions on your eHealth system, this field does not appear in the Edit Element window.
   b. Select a different time zone.
   c. Click OK.
   The Edit Element window closes, eHealth updates the element properties, and Live Exceptions no longer monitors the element.
Modify Properties of a Permanent Virtual Circuit Element

Through the Poller Configuration dialog, you can specify a new agent type, new path components, and a new time zone.

To modify a PVC element

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Poller Configuration.
   The Poller Configuration dialog appears.
3. Select Path/PVC Manager.
   The Path/PVC Manager dialog appears.
4. Select Frame Relay Circuit, select an element, and click Modify.
   The Modify PVC Element dialog appears.
5. Change the properties of the element, and click OK.
   The Modify PVC Element dialog closes and the updated elements appears in the Poller Configuration dialog and the OneClick for eHealth console.

How to Use DCI to Modify Element Information

If you have a network management system (NMS) or other source at your site that collects configuration information and data for your resources, you can use the DataSync application programming interface to import element information and modify it. To use DataSync, you must be comfortable creating programs, scripts, and files that use complex syntax and have a working knowledge of eHealth. For detailed instructions, see the eHealth Data Integration Guide.

To modify element information using DataSync, follow these steps:
1. Use DataSync to import element information.
2. Export the information to a Database Configuration Information (DCI) file.
3. Modify the element properties, and save the file.
4. Import the file into the eHealth database.

Element Removal

Over time, you may remove resources from the infrastructure or determine that you no longer want to monitor them. If you continue to poll elements that do not exist, eHealth may generate "No Response to Ping" polling errors, and future discoveries will list those resources as Missing Elements in the discover log. To keep your database up-to-date, and prevent eHealth from attempting to poll these elements, you must delete or retire them.
Deleting an element is a permanent action. You will not be able to resume polling for that element in the future, and eHealth will no longer include that element in its reports. When you retire an element, you remove it from polling, but eHealth will continue to include it in reports. If you plan to begin collecting data for it again, you should turn off polling for the element rather than retire it.

How to Delete Elements

A deleted element is one that you no longer want to poll and that you do not want to include in reports. When you delete an element, eHealth removes all data associated with that element from the database. However, eHealth could attempt to rediscover it the next time that you run the discover process for the same IP address. As a best practice, if you do not want to rediscover existing elements that you have deleted, add the IP addresses to an IP exclusion file to filter them from the discover. Follow the instructions provided in Exclude Specific Elements from the Search on page 51.

When deleting elements from your database, keep in mind the following:

- If you delete a router element, eHealth also deletes all elements associated with that router, such as CPUs, interfaces, and so on. If the Record detail data option is set for a router element, you can delete its parent and still continue managing the interface.
- If you delete a system element, eHealth also deletes all elements associated with that system, such as CPUs, disks, partitions, interfaces, process sets, and processes. If the Record detail data option is set for a system element, you can delete its parent and still continue managing the interface.
- If you delete a process set, eHealth deletes all of its associated processes as well. If you rediscover the system and choose to find processes, eHealth rediscovers the process set.
- If you delete an application service element, eHealth also deletes all process sets that are associated with that element.

Before you delete an element, follow these steps:

1. Use OneClickEH to right-click it and select Ping from Server.
2. If the element does not respond, confirm that the network has not experienced an outage that could be preventing the element from responding. Ping problems can result from temporary connectivity problems. The element will stop returning ping errors once the network problem is resolved.
3. Once you are certain that the element does not exist and you are sure that you do not want to monitor it, right-click and select Delete, and then click OK.
How to Retire Elements

A retired element is one that you no longer want to poll, but that you want to include in reports until its data ages out or you delete the element. When you retire an element, you retain the old element but do not collect new data for it. You may want to retire an element when you upgrade to a new technology so that you can compare the improvement for the new technology type. The discover process ignores retired elements when it compares newly discovered elements to those in the database.

When you have turned off polling for an element or when data is no longer available for it, you can retire it by right-clicking it and selecting Retire from the OneClickEH menu. Once you have retired an element, eHealth grays out its entry in all OneClickEH element tables. If you want to return a retired element to an active status, right-click the element and select Unretire from the menu.

Note: When you unretire an element that was previously being monitored by Live Exceptions (LE), eHealth does not re-enable LE monitoring. You must use the OneClickEH console to edit the element and re-enable the setting.

When retiring elements, follow these guidelines and practices:

- When retiring a parent element, keep in mind that eHealth automatically retires all related child elements that do not consume their own polling licenses. It does not retire child elements for which you have enabled the Record detail data option.
- If you rediscover a device that has the same name as a retired element, eHealth appends the -A extension to the new element’s name. When this occurs, you should rename the retired element and rediscover the active elements to eliminate the -A extension from the names.

Element Creation

Under most circumstances, the discover process will find all of your resources and add them to your database automatically. In a typical eHealth environment, you should not have to use the eHealth console to manually add elements. However, you may need to manually add elements in the following cases:

- eHealth discover process does not add a statistics element to your configuration automatically.
- The default modem pool element that eHealth creates does not reflect your modem pool configuration, so you need to create modem pool elements and assign the modem and ISDN elements to the correct modem pools.
- You want to add permanent virtual circuit (PVC) elements to your discovered Frame Relay elements.

Add a Statistics Element

If discover does not automatically add a statistics element to your database, you can use the eHealth console to manually add the element.
To add a statistics element

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Poller Configuration.
   The Poller Configuration dialog appears.
3. Click Add.
   The Add Element dialog appears.
4. Do the following:
   a. Specify a unique element name that includes some alphabetical characters.
   b. If you are adding an element that is on a router, system, or remote access server (or part of a modem pool), specify the router, system, remote access server, or modem pool element name as the parent name.
   c. (Optional) Specify the speed, index, and poll rate.
   d. (Optional) If you are adding a router or system interface element, select Record detail data so that eHealth reports on individual statistics in LAN/WAN reports and aggregate statistics in the Router or System reports.
   e. Click OK.
   The Modify Element dialog closes, and eHealth creates the element. At the next scheduled poll, eHealth polls it and updates the Poller Licenses Required information.

Create Modem Pool Element

If the default modem pool element that eHealth creates does not reflect your modem pool configuration, you can create modem pool elements and assign the modem and ISDN elements to the correct modem pools.

To create a modem pool element

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Poller Configuration.
   The Poller Configuration dialog appears.
3. Click Add.
   The Add Element dialog appears.
4. Do the following:
   a. Specify a unique element name.
   b. Select Modem Pool from the Agent Type list.
   c. Specify a parent name that is exactly the same as the element name.
d. Specify a unique combination of an IP address and one or more MIB indexes to uniquely identify the modem pool element. You can specify any combination of values. For example, you could use the same IP address for all of your modem pools and change the MIB index values to uniquely identify each modem pool.

e. Click OK.

The Modify Element dialog closes, and eHealth creates the element.

5. In the Poller Configuration dialog, select one or more modem or ISDN elements and click Modify.

The Modify Element dialog appears.

6. In the Change Parent to field, specify the modem pool element name and click OK.

The Modify Element dialog closes, and eHealth associates the selected elements to the same pool.

Add a Permanent Virtual Circuit Element for a Frame Relay Element

After discovering Frame Relay elements, you can add PVC elements using the Poller Configuration dialog. With the exception of the path components, the information is similar to the properties that you specify for a statistics element.

To add a PVC element

1. Log in to the eHealth console as an administrator.

   The eHealth console appears.

2. Select Setup, Poller Configuration.

   The Poller Configuration dialog appears.

3. Select Path/PVC Manager.

   The Path/PVC Manager dialog appears.

4. Select Frame Relay Circuit and click Add PVC.

   The Add PVC Element dialog appears.

5. Complete the fields to define the element and click OK.

   The Add PVC Element dialog closes, the elements appears in the Poller Configuration dialog, and the OneClick for eHealth console.
Chapter 5: Organizing Your Element Configuration by Grouping

This chapter contains the following sections:

- The Grouping Capability
- Group and Group List Creation
- Group Management

The Grouping Capability

eHealth provides a grouping capability that enables you to organize related eHealth elements to manage your infrastructure based on the geographic region, customer, organization, or department that they support. By focusing on a subset of elements—rather than all elements in your infrastructure—you can facilitate eHealth administration and simplify reporting. For example, if you wanted to monitor the systems supporting your business within Europe, you could create a group called England (composed of systems that support offices in that country), another group called Germany, and a third group called Italy. You could then add those groups to a group list called Europe and generate report data on the entire group list. eHealth offers flexible grouping. Elements can belong to multiple groups, and groups can belong to multiple group lists.

To group elements, you can use any of these methods:

- **DCI** - If you use eHealth’s DataSync application programming interface to import your element information, you can create DCI files to define your groups. For instructions, see the eHealth Data Integration Guide.

- **Discover** - You can automatically add elements to new or existing groups as you discover the elements.

- **CLI** - At the command line, you can run nhGroup to create a new eHealth group and add elements to it. For instructions, see the eHealth Commands and Environment Variables Reference Guide.

- **OneClickEH** - Using the Managed Resources feature in the OneClickEH console, you can select all elements that you want to add to a group and right-click to add them, or you can drag and drop them from an element list into the designated group.
How to Use OneClickEH to Create a Group of Elements

As soon as you discover elements, eHealth creates a default group called All that includes the elements that it found. You can simplify reporting by associating related elements to groups based on the geographic region, customer, organization, or department that they support. eHealth offers flexible grouping. Elements can belong to multiple groups. If your web user account has permission to manage groups, you can use OneClickEH to organize subsets of your elements into specific groups.

To create a group of elements, do the following:
1. Identify the elements that you want to include.
2. Add the elements to the group.
3. Assign a name to the group by following the eHealth naming restrictions.
4. Enable other administrators to view the groups by modifying their user accounts.
5. (Optional) Enable the SmartTree feature for those administrators to allow them to view the groups in a hierarchy based on the naming convention that you used.

Group and Group List Creation

eHealth offers flexible grouping. Elements can belong to multiple groups, and groups can belong to multiple group lists. The OneClick for eHealth console allows you to dynamically create groups of related elements, and then add the groups to group lists based on function or location. Using the eHealth Web user interface, you can automatically generate reports against groups and group lists that you create yourself.

You can automatically generate reports through the eHealth web user interface against groups that you create yourself. To allow other administrators to view reports against groups that you or other users created, you must modify the permissions on the user account to give the user access to those subjects. If you want to limit an administrator’s visibility to certain resources, you can give the administrator selected group access (allowing the administrator to administer only a subset of elements).

Create a Group Using the OneClick for eHealth Console

Using the OneClick for eHealth console, you can dynamically create groups of related elements, and then view reports based on the performance data collected on the resources within the groups. To view reports based on groups that were created by other administrators, your web user account must have the appropriate permission to do so.
To create a new group

1. Open the OneClickEH console.
   a. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups and web users.
   b. In the left pane, select Managed Resources, Groups.

2. Identify the elements that you want to include and add them to the group:
   a. In the left pane, select Managed Resources, Elements.

   The element table appears.
   b. Click Go to display all elements in your configuration, or select the Elements tab to filter the list. Include a wildcard such as an asterisk (*) to match characters, or a question mark (?) to match a single character.

   The table refreshes to display the specified elements.
   c. Identify any other groups to which each element belongs. Double-click each element name and select the Group Membership tab in the Edit Element window.

   The list of groups to which the element belongs appears.
   d. Select all elements that you want to include, right-click, and select Create Group with Selected Elements.

   The Create Group window appears.

3. Specify the group name and a description, and click OK. Be sure to adhere to these restrictions:
   - Always use a unique name for each group. Due to eHealth naming restrictions, you cannot create two groups with the same name.
   - Use a maximum of 64 single-byte or 32 double-byte characters using uppercase or lowercase letters, the numbers 0 through 9, periods (.), dashes (-), and underscores (_).
   - Do not use all numbers, and do not include the word All, FirstSense, forward slashes (/), or spaces.
   - (Optional) Use a naming convention that reflects the location or function of the elements. Append a label to the group name and use a delimiter (for example: Boston-1, Atlanta-1, or Chicago-1).

   The group immediately appears under By Group.

4. Repeat Steps 2 and 3 to create other groups with the same suffix. For example: Boston-2, Atlanta-2, Chicago-2.

   The new groups appear in the tree.

5. (Optional) Add additional elements to the groups:
   a. In the Groups window, select the Elements Not in Any Group tab to identify resources that you have not yet associated to any groups.
   b. Drag and drop one or more of these elements into one or more of the groups in the tree.

   OneClickEH adds the selected elements to the specified groups.
6. Enable other administrators to view the groups that you have created:
   a. In the left pane, select User Administration.
      The User Administration window appears.
   b. Double-click the user account name.
      The Modify User window appears.
   c. Select the Groups tab.
   d. Select All or choose the specific groups that you want the administrator to view, and then click OK.
      OneClickEH updates the permissions on the specified user account.

**Virtual Grouping**

If the SmartTree feature is enabled for a web user account, OneClickEH displays eHealth groups in a hierarchy based on the naming convention that the user employed rather than displaying them in basic alphabetical order. By default, this feature is enabled for the primary administrator account. You must enable it for individual administrator accounts by selecting the SmartTree tab on the User Administration page.

For example, if you name groups using a format such as location-organization to indicate the geographic regions in which the elements reside and the departments that they support, OneClickEH displays them in a logical hierarchy in the left pane, creating “virtual” groups based on the naming convention.

For example:

Atlanta
   finance (3)
   sales (3)
   marketing (5)

Boston
   finance (4)
   sales (3)
   marketing (3)

In this example, Atlanta and Boston appear in the World View as “virtual” groups to reflect the grouping hierarchy. Although you did not actually create the groups Atlanta and Boston, OneClickEH assumes, based on the use of hyphens in the names, that this is the appropriate grouping hierarchy and creates it. It also labels each group with the total number of elements that it contains. If the SmartTree feature was not enabled for this account, the group names would appear in alphabetical order in the left pane of the console and the groups Atlanta and Boston would not appear.
Create a Group List Using the OneClick for eHealth Console

Using the OneClick for eHealth console, you can dynamically add groups to group lists, and then view reports based on the performance data collected on the resources within the group lists. Groups can belong to multiple group lists.

**Note:** To view reports based on group lists that were created by other administrators, your web user account must have the appropriate permission to do so. If a user account has access to a group list, the account has implicit access to all groups and elements contained within it.

If you want to limit an administrator’s visibility to certain resources, you can modify the permissions on the user account to give the administrator selected group list access to administer only a subset of group lists.

**To create a new group list**

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
2. Identify the groups that you want to include and add them to the group list:
   a. In the left pane, select Managed Resources, Groups.
      The Groups window appears.
   b. Identify any other group lists to which each group belongs. Double-click each group name and select the Group List Membership tab in the Edit Element window.
      The list of group lists to which the group belongs appears.
   c. Select all groups that you want to include, right-click, and select Create Group List with Selected Groups.
      The Create Group List window appears.
3. Specify a name and a description. Adhere to these restrictions:
   - Always use a unique name for each group list. Due to eHealth naming restrictions, you cannot create two group lists with the same name.
   - Use a maximum of 64 single-byte or 32 double-byte characters using uppercase or lowercase letters, the numbers 0 through 9, periods (.), dashes (-), and underscores (_).
   - Do not use all numbers, and do not include the word All, FirstSense, forward slashes (/), or spaces.
4. (Optional) Enable the group list to be visible in the BSC.
5. Click OK.
   The console refreshes, and the new group list appears in the tree.
6. (Optional) Add additional members to the group list:
   a. Double-click the group list name under Group Lists, and select the Groups Not in This Group List tab.
   b. Scroll through the list to find the groups that you want to include.
Group Management

The OneClick for eHealth console allows you to dynamically modify group and group list membership, change the properties of groups and group lists, remove groups and group lists from the database, and rename them.

Change Group Membership

At any time, you can add new members to a group or remove members. The OneClickEH Group window identifies all elements that the group contains, all elements that are not associated to any group, and all elements that are not in the group.

Important! If you created a group on a remote polling site, you cannot edit it from the central site. You must log in to the remote polling site in your OneClickEH World View to make your changes.

To change group membership

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
2. In the left pane, select Managed Resources, Groups.
   The tree expands to show the list of groups available.
3. Double-click a group name and select the Elements tab.
   The Elements window appears.

   c. Quickly identify the group lists to which each group belongs by right-clicking the group name and selecting the Group Membership tab.
   d. Select all groups that you want to include, right-click, and select Add Selected Groups to Group List.
      OneClickEH adds the groups to the group list.
7. Enable specific users to view the group lists that you have created:
   a. In the left pane, select User Administration.
      The User Administration window appears.
   b. Double-click the user account name.
      The Modify User window appears.
   c. Select the Group Lists tab.
   d. Select All or choose the specific group lists that you want the administrator to view, and then click OK.
      OneClickEH updates the permissions on the specified user account.
8. View the group lists by selecting Managed Resources, Group Lists.
4. Click Go.
   OneClick displays all elements that are contained in that group.

5. Add new members to the group. Select the Elements Not in This Group tab and click Go.
   OneClick displays all elements that are not contained in the group.

6. (Optional) Select the elements that you want to add, right-click, and select Add Selected Elements to Group.
   OneClickEH adds the elements to the group.

7. (Optional) Remove members from the group. Select the Elements tab and click Go.
   OneClickEH displays all elements contained in the group.

8. Select the elements that you want to remove, right-click, and select Remove Selected Elements from Group.
   OneClickEH removes the elements from the group.

Change Group List Membership

At any time, you can add new members to a group list or remove members. The OneClickEH Group List window identifies all groups that the group list contains, all groups that are not associated to any group list, and all groups that are not in the group list.

**Important!** If you created a group list on a remote polling site, you cannot edit it from the central site. You must log in to the remote polling site in your OneClickEH World View to make your changes.

To change group list membership

1. **Access the OneClickEH Console** and log in to the eHealth system as an administrator who has permission to manage groups.

2. In the left pane, select Managed Resources, Group Lists.
   The Group Lists window displays the names of the existing group list.

3. Double-click a group list name.
   In the right pane, OneClickEH displays all groups that are contained in that group list.

4. Do any of the following:
   - Add new members to the group list. Select Groups Not in This Group List tab, select the groups that you want to add, right-click, and select Add Selected Groups to Group List.
   - Remove members from the group list. Select the Groups tab, select the groups, right-click, and select Remove Selected Groups from Group List.
Renaming a Group

You can rename a group at any time. However, you cannot specify the name of a group that you recently deleted. If you want to reuse a group name immediately after removing it, you must clean up the soft-deleted group row in the database.

To rename a group

1. If you recently deleted a group and you want to use that group name again, run the following command at the command line:

   `nhScrubFsa -fsaTtl 0 -deleteObjectHours 0`

   eHealth removes the file from the database.

2. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.

3. In the left pane, select Managed Resources, Groups.

4. Double-click the group name, or right-click and select Edit Group. The Modify Properties window appears.

5. Specify a new name, and click OK. OneClickEH displays the new name in the left pane.

Renaming a Group List

You can rename a group list at any time. However, you cannot specify the name of a group list that you recently deleted. If you want to reuse a group list name immediately after removing it, you must clean up the soft-deleted group list row in the database.

To rename a group list

1. If you recently deleted a group list and you want to use that group list name again, run the following command at the command line:

   `nhScrubFsa -fsaTtl 0 -deleteObjectHours 0`

   eHealth removes the file from the database.

2. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.

3. In the left pane, select Managed Resources, Group Lists.

4. Double-click the group list name, or right-click and select Edit Group List. The Modify Properties window appears.

5. Specify a new name, and click OK. OneClickEH displays the new group list name in the left pane.
Copy a Group List

If you want to create several group lists composed of the same members, you can copy a group list rather than create each one manually.

To copy a group list

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
2. In the left pane, select Managed Resources, Group Lists.
   The right window refreshes and then displays the existing group lists.
3. Right-click the group list name, and select Copy Group List.
   The Create a New Group List window appears.
4. Specify a name and description.
5. (Optional) Do the following:
   a. Select Groups to include the same groups.
   b. Select Live Profiles to associate the same Live Health profiles.
   c. Select users to allow the same users to access it.
   d. Select Visible in Business Service Console to display it in the BSC.
6. Click OK.
   The Modify Properties window closes, and the new group list appears in the pane.

Copy a Group or Group List

If you want to create several groups composed of the same members, you can copy a group rather than creating each one manually. You can also copy a group list.

To copy a group or group list

1. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
2. In the left pane, select Managed Resources, Groups (or Group Lists).
3. Right-click the group name (or group list name), and select Copy Group (or Copy Group List).
   The Create a New Group (or Create a New Group List) window appears.
4. Specify a name and description.
5. (Optional) Do the following:
   a. Select Elements (or Groups) to include the same elements (or groups).
   b. Select Live Profiles to associate the same Live Health profiles.
   c. Select users to allow the same users to access it.
   d. Click OK.
   The Modify Properties window closes, and the new group or group list appears in the tree.
Remove a Set of Groups from the Database

If you determine that you no longer need to monitor specific groups of elements, you can delete them. However, before you do so, delete any scheduled reports that use the group, and move any associated elements to another group.

To remove a set of groups

1. (Optional) If you intend to reuse the group names immediately, rename the groups by doing the following:
   a. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
   b. In the left pane, select Managed Resources, Groups.
   c. Select the first group, double-click it, specify a new name in the Modify Properties window, and click OK.
   d. Repeat Step c to rename each of the other groups.
      
      Note: If you skip this step, but you want to reuse a group name immediately, you must perform Step 10 to force the removal of the file from the database.
      
      The Modify Properties window closes, and eHealth displays the new group names.

2. Log in to the eHealth console as an eHealth administrator.
3. Select Setup, Options.
   
   The Options dialog appears.
4. Specify the names of the groups in the Set Element Filter field, and click OK.
   
   The Options dialog closes.
5. Select Setup, Poller Configuration in the eHealth console.
   eHealth displays the elements for the selected groups only.
6. In the Poller Configuration dialog, select all elements and click Delete.
   eHealth removes all elements from the dialog.
7. Click OK.
   
   The Poller Configuration dialog closes.
8. Select Setup, Schedule Jobs in the eHealth console.
   The Schedule Jobs dialog appears.
9. Do the following:
   a. Sort the jobs by subject, or use another method.
   b. Carefully select those scheduled report jobs that apply to the groups and/or elements that you are removing only.
   c. Click Delete to remove all scheduled jobs for the groups.
   d. Click OK.
   The Schedule Jobs dialog closes.
10. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.

11. Do the following:
   a. Click Managed Resources, Groups.
   b. Right-click inside the element table.
   c. Select Select All from the pop-up menu.
   d. Select Delete Selected Groups.
   e. Health removes the groups from the list.

12. (Optional) If you did not perform Step 1 of this procedure, and you need to reuse the group names immediately, specify the following at the command line:

```
nhScrubFsa -fsaTtl 0 -deleteObjectHours 0
```

### Remove a Set of Group Lists from the Database

If you determine that you no longer need to monitor specific group lists of elements, you can delete them. However, before you do so, delete any scheduled Service Level reports that use the group lists, and move any associated groups to another group list.

#### To remove a set of group lists

1. (Optional) If you intend to reuse the group list names immediately, rename the group lists by doing the following:
   a. Access the OneClickEH Console and log in to the eHealth system as an administrator who has permission to manage groups.
   b. Click Managed Resources, Group Lists.
   c. Select the first group list, double-click it, specify a new name in the Modify Properties window, and click OK.
   d. Repeat Step c to rename each of the other group lists.
   **Note:** If you skip this step, but you want to reuse a group list name immediately, you must perform Step 10 to force the removal of the file from the database.
   e. The Modify Properties window closes, and eHealth displays the new group list names.

2. Select Setup, Schedule Jobs in the eHealth console.
   The Schedule Jobs dialog appears.

3. Do the following:
   a. Carefully select those scheduled Service Level report jobs that apply to the group lists that you are removing only.
   b. Click Delete.
   c. Click OK.
   The Schedule Jobs dialog closes and eHealth removes all scheduled jobs for the group lists.
4. **Access the OneClickEH Console** and log in to the eHealth system as an administrator who has permission to manage groups.

5. Do the following:
   a. Click Managed Resources, Group Lists.
   b. Right-click inside the table.
   c. Select Select All from the pop-up menu.
   d. Select Delete Selected Group Lists.
   e. Health removes the group lists from the list.

6. (Optional) If you did not perform Step 1 of this procedure, and you need to reuse the group list names immediately, specify the following at the command line:
   
   ```
   nhScrubFsa -fsaTtl 0 -deleteObjectHours 0
   ```

**Filter Display to Show Elements in a Specific Group Only**

If you manage a large number of elements, it might be difficult to focus on a specific set of related elements. If you use groups to organize your elements by location, type, department, or customer, you can specify a group name in the Set Element Filter field (without wildcards) to show only the elements in a specific group when you edit elements or run reports from the console.

**Note:** This option does not filter probe elements for the Traffic Accountant application. eHealth displays all probe elements, regardless of the Set Element Filter setting.

**To set an element filter**

1. Log in to the eHealth console as an eHealth administrator.
2. Select Setup, Options.
   
   The Options dialog appears.
3. Select the Set Element Filter field and do one of the following:
   a. Specify a group name (without a wildcard), and then click OK.
   b. Click Browse, select a group name from the list of existing groups, and click OK.
   
   The Options dialog closes.
4. If you specified a group name in Step 3 that does not currently exist, create the group by using the OneClickEH grouping feature or specify the Group option when you run an interactive discover.
Chapter 6: Configuring eHealth User Account Permissions

This chapter contains the following sections:

- Web User Account Permissions
- Create a Web User Account
- Set OneClickEH Admin Permissions

Web User Account Permissions

To access the web user interface and manage eHealth systems using OneClickEH, a user must have an eHealth web user account. To perform most functions from either interface, a user needs to have the appropriate account permissions. Web user account permissions control the user's access to web user interface pages, eHealth applications, reports, and administrative functions. However, a standard default account does not provide access to all of the features available.

By default, eHealth web administrators can access all administrative functions available with OneClickEH. You cannot disable access to OneClickEH for the admin account or disable permission to manage web user accounts. These permissions are permanently enabled for the admin user.

Create a Web User Account

If you have an admin account, or another administrator gives your account permission to manage user accounts, you can enable other web users to access the web interface and OneClickEH. You can either create a standard web user account with default permissions or copy an existing account.

To create a standard web user account with default permissions

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click User Administration and select New User.
4. Specify a user account name. Follow these guidelines:
   - Do not use forward slashes (/) in the name.
   - You can use Latin characters (within unicode range 21-FF); however, spaces, tabs, and the following characters are not supported: ~ ` ! @ # % ^ & * ( ) + = [ ] {} | : ; ' " , < > / ? \ 
5. Specify a password that the web user must use to log in to the Web user interface. By default, every user must supply a web user name and password to log in to an eHealth system from OneClickEH. If you do not specify a password for the account, the web user will not be required to specify a password to access the web user interface.
   **Note:** Specify 0 to 9 characters, and then respecify the characters again in the Reype Password field. Valid characters include the letters a through z (uppercase and lowercase) and the numbers 0 through 9.
6. (Optional) Change the default account settings by selecting the appropriate tab on the left.
7. Click OK.

After the screen refreshes, the new user account name should appear in the User Account list.

**Copy Web User Account**

If you need to create several user accounts with similar permissions, you can copy the settings of an existing web user account.

**To copy a web user account**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click the user name in the list and select Copy User.
   The Copy User page appears.
4. Specify a user account name and password, and then click OK.
   OneClickEH creates the new account and displays it in the User Account list.

**Delete Web User Account**

If you no longer need a web user account, you can delete it; however, you cannot delete the admin account.

**To delete a web user account**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click the user name in the list and select Delete User.
   A confirmation dialog appears.
4. Click OK.
   OneClickEH removes the account name.

**How to Change Web User Account Permissions**

By setting specific permissions on a web user account, you can control the user's access to various web pages, eHealth applications, and reports. You can also limit the administrative functions that the user can access through the web user interface and OneClickEH.

**Important!** If you modify, disable, or enable permissions on a web user account while the user is logged in, some changes may not take effect immediately. As a result, options that have been disabled may still appear in the menus. If a user attempts to use an option that you have disabled, an error will occur. To effect all changes immediately, the user must log out of OneClickEH and log back in.

By default, eHealth web administrators can access all administrative functions available with OneClickEH. You cannot disable access to OneClickEH for the admin account or disable permission to manage web user accounts. These permissions are permanently enabled for the admin user.

By default, web users do not have access to any OneClickEH functions, but they are given access to some functions that are available through the eHealth Web user interface. If a user is unable to access an eHealth feature or administrative function, you can change the permissions associated with the user account.

To change web user account permissions, do the following:

1. **Access the OneClickEH Console** and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. Open the account page for the web user account that you want to change.
3. Select each tab on the left to set or reset the permissions associated with the account, and click OK.
4. Advise the user to log out and log back in to effect the changes.
5. If you changed any permissions associated with the Live Exceptions application, advise the user to close the Live Exceptions Browser window to allow the changes to take effect.
6. If you changed any permissions associated with MyHealth reporting, confirm that the web user’s browser is updating pages rather than using old versions of pages saved in cache.
Set OneClickEH Admin Permissions

By default, eHealth web administrators can access all administrative functions available with OneClickEH. You cannot disable access to OneClickEH for the admin account or disable permission to manage web user accounts. These permissions are permanently enabled for the admin user. By default, web users do not have access to any OneClickEH functions. You must enable access to each function by selecting the OneClickEH tab on the User Administration page.

To set OneClickEH permissions for a user account

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click the user name in the list and select Edit User.
4. Select the OneClickEH tab, and then select Yes next to User can access OneClick for eHealth.
5. (Optional) Allow the user to do any of the following:
   - Add, delete, or modify eHealth web user accounts.
   - Manage elements by accessing all options available in the element actions pop-up menu.
   - Modify the read-write and read-only community strings pertaining to the elements.
   - Add, delete, copy, and modify groups and group lists.
   - Modify Traffic Accountant views and groups.
   - Access the Polling Management interface to review and resolve polling errors.
   - View the various logs available in the eHealth History folder.
   - Access the Job Scheduler folder to view scheduled jobs.
   - Access the System Information folder to view the status of the database, server processes, environment variables, license keys, and eHealth files.
   - Access the Setup folder to manage the eHealth system and pollers, and perform advanced logging to troubleshoot eHealth configuration problems.
6. Click OK to update the account.

Set General Permissions

By selecting the General tab on the User Administration page, you can set the following miscellaneous account permissions:

- Specify a user alias name to appear in the upper-right portion of the Business Service Console (BSC) screen next to User. This name appears in place of the eHealth web user account name.
- Provide a description of the web user (the default is New User).
- Prevent the user from being able to access the Change Password administrative function on the Administration page in the eHealth Web user interface.
- Allow the user to specify a time zone for reports that are generated from the eHealth Web interface.
- Specify the time zone on which eHealth should base reports. By default, eHealth runs reports for the time zone of the eHealth system.
- Show alias names instead of element names for elements in reports run from the web user interface and in web pages (such as the Run Reports, Organization, and Report List pages).
- Limit the user's viewing access to specific reports saved in a web directory. Allow the user to delete element-based reports on demand from the Organization or Report List pages.

**Change the User Account Password**

If you set the User can change password option to Yes on the General page, a user can change the account password at any time from the Administration page of the eHealth Web user interface. As an administrator, you can change the password for the account at any time by selecting the Password tab on the User Administration page.

**Enable Access to the Web Interface Tabs**

By default, eHealth allows a user to view all tabs on the eHealth Web user interface and displays the Organization page as the initial viewing page. By selecting Web Tabs on the User Administration page, you can disable access to one or more web interface pages. If you turn off the display of a page, the tab does not appear in the navigation bar and the user does not have access to any of the options on that page. You can also change the initial viewing page by selecting a page name from the Default tab list.

**Enable Access to BSC & Live Features**

By selecting the BSC & Live tab on the User Administration page, you can give the user permission to do the following:

- Access Live Trend.
- Ability use fast sampling.
- Access the Live Exceptions Browser, or administrative permission to create, modify, and delete profiles, and monitor subjects with those profiles.
- In the Live Exceptions Browser, view acknowledgements only, or acknowledge an alarm and view acknowledgements. To unacknowledge an alarm, a user must have administrator privileges and the ability to edit acknowledgements.
- In the Live Exceptions Browser, view annotations, or view annotations and annotate an alarm.
**Important!** For a user account on a Distributed eHealth Console, you can enable the display of the DE System column in the Live Exceptions Browser event table. This column appears in the event table on Distributed eHealth Consoles. It lists the names of the Distributed eHealth Systems on which the Live Exceptions application has generated an alarm.

- Access Live Status.
- Access the BSC.

Through the BSC & Live page, you can also configure the following for a particular user account:

- Frequency with which eHealth refreshes the Live Exceptions Browser and the Live Status display. (This refresh rate does not apply to Live Trend.) The default refresh rate is five minutes. If you have an eHealth Live Health Fault Manager license, you can change it to one or two minutes.
- Percentage of alarms that must be acknowledged for a system, application, or network device before the BSC will display a checkmark in a dashboard view.
- Permission for the user to view notes if the user is included in the note’s Reader list, allow the user to create and modify notes, or give the user access to notes, regardless of the domain to which you add the user. By default, a user can view Service Notes if the user is a BSC administrator, the owner of the note, or the creator of the note.

**Note:** After you modify a user account, advise the user to close the Live Exceptions Browser window to allow the changes to take effect.

### Set Report Shortcut Preferences

By default, eHealth allows web users to run At-a-Glance, Top N, and Trend reports from the Organization page. The Preferences feature on the Administration page of the eHealth Web user interface allows users to specify their own saved Run Report screen shortcuts instead of the standard screens.

**To prevent a user from changing preferences**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click the user name in the list and select Edit User.
4. Select the Preferences tab, and then select No next to User is allowed to change preferences.
5. Click OK.

When the user logs in to the eHealth Web user interface, the Preferences feature does not appear on the Administration page.

**Note:** From this page, you can also select other Run Report screens for the user.
Set MyHealth Report Permissions

To enable web users to design the panels and content of their MyHealth reports, you must give their accounts the appropriate permissions. If you change the MyHealth permissions for a web user account or create a new MyHealth report, the changes might not appear immediately. Check to confirm that the web user’s browser is updating pages rather than using old versions of pages saved in cache.

To set MyHealth report permissions

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Right-click the user name in the list and select Edit User.
4. Select the MyHealth tab, and set any of the following permissions:
   - Increase the number of MyHealth reports that the user can run nightly. By default, eHealth allows the user to run five MyHealth reports nightly.
   - Allow the user to run MyHealth reports on demand. If you allow the user to run reports on demand, the user can still only run five reports on demand as well.
   - Prevent the user from being able to edit the contents of a MyHealth report.
   - Control the types of reports that a user can include in a MyHealth report.
   - Change the default greeting that initially appears when creating a MyHealth report.
5. Click OK.

Enable Access to TA Views

By selecting the TA tab on the User Administration page, you can allow the user to generate and view all Traffic Accountant reports for all nodes without any restrictions, or disallow any access to views.

Set Reporting Permissions

By default, a web user account allows the user to run all report types. By selecting the Reports tab on the User Administration page, you can set the following types of permissions for a user account:

- Prevent the user from running reports from the Run Reports page of the Web user interface and running drilldown reports of that type.
  
  **Note:** The At-a-Glance, Trend, and Element Configuration drilldown options do not appear in the OneClickEH pop-up menu for a user unless the web user account has permission to run these reports.

- Enable the user to customize web reports by modifying presentation attributes through each Run Report screen.

- Enable the user to save report settings as a customized report.
Limit the user's ability to run reports based on their name. To specify more than one name, separate each name with a space. To restrict the user to template names containing specific text, specify the text or a regular expression followed by the * symbol. For example, specify Blue* to permit the web user to run default reports and customized report templates with names that begin with Blue.

**Important!** This option applies to system templates that you create for the entire site; it does not apply to templates that users create for themselves.

### Set Agent Management Permissions

By selecting the Agents & AVie View tab on the User Administration page, you can give a user permission to access the following AdvantEDGE View and agent management features:

- View, create, and delete tables and queries in AdvantEDGE View.
- Global AdvantEDGE View preferences and display configuration and diagnostic information.

**Important!** The Admin option automatically gives the web user the ability to view tables and queries in AdvantEDGE View, as well as the ability to modify, create, and delete table rows.

- Application Response management functions.
- Drill down from a Live Health application or a report to the Application Response Agent Transaction Viewer.
- Service Availability agent management functions.

### Enable Access to Groups and Group Lists

You can automatically generate reports from the eHealth Web user interface against groups and group lists that you create yourself. If you are logged in as an eHealth web administrator, you can view all reports for all subjects being monitored by the eHealth system.

To enable a user to view reports against groups and group lists created by other users, the user account must have access to those subjects. To determine which users have access to a group or group list, select the group name in the left pane, and then select the Users Access tab in the Group or Group List window.

**To set group and group lists permissions**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage web user accounts.
2. In the left pane, select Tasks and Information, User Administration.
3. Double-click the user account name.
4. Select the Groups or Group Lists tab.
5. Select All or select specific groups or group lists that the user can view.
6. Click OK or update the account.
Chapter 7: Database Management

This chapter contains the following sections:

- The eHealth Database
- The Role of the eHealth Database Manager
- eHealth Database Backups

The eHealth Database

eHealth includes an integrated database that stores the wide variety of information collected from your IT infrastructure. This repository allows you to run historical reports for your resources. The Oracle database is installed as part of the eHealth installation. For information on installing eHealth, see the eHealth Installation Guide.

The eHealth installation program provides you with the flexibility to create an eHealth database that best fits your organization. You can do the following:

- Use the eHealth database defaults (recommended for most sites) so that eHealth uses proprietary algorithms to determine the best way to set up your eHealth database for maximum performance.
- Create a system sizing file that helps the installation program determine the best way to set up your eHealth database for maximum performance.
- Create a layout configuration file to specify exactly how you want the installation program to configure your eHealth database. Only experienced Oracle database administrators who want to tune the eHealth database to meet the specific needs of their organization should use this option. For more information, see Appendix H: Database Layout File.

The eHealth database is a sophisticated relational database application based on Oracle®. It supports the industry-standard Structured Query Language (SQL), an English-like programming language used to retrieve information and update a database.
The Oracle database consists of datafiles, which are physical structures that store all of the data in the database. A tablespace consists of one or more of these datafiles. Tablespaces are logical storage units within the database that can have tables, indexes, and other internal structures mapped to it. The eHealth database contains a number of tablespaces over several disks. The initial size of the tablespaces is determined by the number of polled elements and the data rollup schedule used to calculate the size of your eHealth database.

Oracle databases also use redo logs and archive logs. Redo logs store data about transactions that alter database information; they are used to restore transactions after a system crash or other system failure. Archive logs are archived copies of redo logs; they provide the capability to recover to a specific point in time for any tablespace in the database. While the Oracle installation enables archive logs, the eHealth software maintains them.

The terms database and instance are often used interchangeably. The largest area of an Oracle installation is the database. To access an Oracle database, you must first have at least one instance of Oracle assigned to that database. An instance is a collection of programs that manage the disk space and tablespaces. When you install Oracle, you are installing an Oracle instance for the eHealth database.

When you save the results of a discover process, eHealth creates an entry in the database for each element that the discover process found. After each poll, eHealth saves the collected data for each discovered element in the database.

The eHealth database contains the following types of data:

- **Element information** – Data that identifies each business resource that you want to manage.
- **Statistics data** – Performance data for resources such as LAN /WAN interfaces, Frame Relay circuits, routers, switches, systems, remote access elements, ATM elements, and response elements.
- **Conversations data** – Performance data for user and application traffic across the network (used by eHealth Traffic Accountant).
- **Live Exceptions data, rules, alarms and calendars** – Data for real-time detection and reporting of faults, potential outages, and delays.

**The Role of the eHealth Database Manager**

Since the eHealth database is fully integrated, it does not require a dedicated database administrator to operate. However, it is important to monitor the database software to confirm that it is running smoothly, and back up the data regularly. In addition, you need to manage the growth of the database so that it does not run out of disk space. eHealth offers various tools that you can use to automate database management tasks.
Follow these best practices as you use the Oracle database:

- Do not install any Oracle patches on your eHealth system. Oracle patches are often not required for the embedded Oracle database within eHealth. Any patches that are required for the eHealth database will be made available as part of an eHealth service pack release.
  
  **Important!** CA provides services and support only for the database version that shipped with eHealth and only if the database software is in the same state in which it was shipped by CA.

- Do not use Oracle tools or other third-party software to back up the eHealth database. You must back up your database using the eHealth save and load utilities.

- Never back up database files using third-party software. Doing so can corrupt the eHealth database.

- Do not make any performance upgrades to your Oracle database. Even if you have an experienced database administrator on site, you cannot modify the embedded Oracle database. The embedded Oracle license does not allow such upgrades. If you experience performance issues, contact Technical Support.
  
  **Important!** Technical Support cannot support an eHealth database if you have performed customizations, unless those customizations have been performed by or through CA, through the use of a CA authorized toolkit, or with express written authorization from CA.

### eHealth Database Sizing

The eHealth Sizing Wizard is a web-based tool that helps you determine the disk space and memory requirements for your eHealth system, including the eHealth database. Use the eHealth Sizing Wizard before you install or upgrade an eHealth release to make sure that your system has adequate resources for the database, and to configure your database layout to optimize performance.

The eHealth Sizing Wizard is available on the eHealth Support web site at the following location:

http://www4.concord.com/sizing/swiz

The three most important factors in planning your database are the number of elements that you intend to monitor, the number of days of as-polled data that you intend to retain, and the number of disks on which you will save the database.

- The number of polled elements determines the initial size of the tablespaces created in the eHealth database. The initial tablespace sizes are designed to optimize performance. Consider the following recommendations:
  - Use the sizing wizard’s popup calculators to accurately count the number of elements for each element type.
  - If you anticipate that the number of elements within your infrastructure will grow quickly, specify the total number of elements that you intend to monitor so that eHealth has sufficient disk space available as the database grows.
In environments without Storage Area Networks (SANs), the eHealth database requires a number of tablespaces over several disks. For optimal performance, you should use as many disks as your budget allows and put each directory on a different device. Consider the following recommendations:

- Several small disks are better than one large disk because data access is much faster.
- For optimal redundancy of critical database files, use at least three disks.

### How to Monitor Disk Space Allocated for Backups

After you schedule incremental saves to begin, check the amount of free disk space remaining on the disks where the backups reside. You must monitor the disk space that the backups consume because a filled disk causes the save to fail. Also, when you initially set up an incremental save strategy, it is important to determine how much space the level 0 and level 1 saves require. This planning information is valuable if you decide to change the frequency of saves or the backup locations. If you recently installed eHealth, the initial saves will be smaller and grow over time as the database fills with as-polled and rolled-up data. For example, if eHealth saves 30 days of as-polled data, the database will not be full for at least 30 days.

To monitor disk space for backups, follow these steps:

1. Install a system agent such as the Unicenter NSM or eHealth SystemEDGE agent. The agent monitors disk space on the devices on which you back up the eHealth database. It also informs you when errors and failures occur with job log files, and when disk space reaches a certain threshold, such as 75%, so that you can take steps to acquire more disk space.
2. Proactively manage the size of backups. Run the `nhSaveDbConfig` command with an argument that allows you to display the amount of disk space used by each scheduled save:

   ```
   nhSaveDbConfig -listSizes
   ```

3. After you install and configure an agent, and discover your eHealth system, report on eHealth database performance metrics by running eHealth At-a-Glance reports for Oracle application service elements. These reports include charts on useful Oracle metrics such as its CPU utilization, disk usage, commits, and rollbacks.
4. (Optional) Configure log file monitoring to enable the SystemEDGE agent to alert you when errors and warnings occur in the eHealth log files. This will allow you to resolve issues before problems impact database performance.

**Important!** For instructions on installing and configuring the SystemEDGE agent and eHealth AIM for Oracle, see the *eHealth SystemEDGE User Guide* and the eHealth Help. For information on using the Unicenter NSM system agent with eHealth, see How to Configure eHealth to Collect Data from Unicenter NSM System Agents on page 171.
Check Disk Space

Datafiles—physical structures that store data in the eHealth database—automatically grow as needed until they reach 32 GB or until the disk does not have enough free space. A tablespace is a logical storage unit that can contain datafiles within an Oracle database. To make sure that your database can accommodate all of the datafiles and tablespaces that support your eHealth system, you can periodically check the database status by using OneClickEH.

If your web user account has the necessary permissions, you can do the following:

- Access the Database Status feature within the System Information folder to view the contents of the entire eHealth database and the times at which the statistics rollups occurred. You can review the size and consumption of each tablespace, and the size and status of the disk partitions and datafiles.
- Review the times at which eHealth rolled up as-pollled, rolled-up, and rolled-up top conversations, and the size of these rollups. (To access this information, you must install an eHealth Traffic Accountant license.)
- Drill down to the Database Alerts message window to identify when problems occurred. You can also drill down to the Job History window to review when all database-related scheduled jobs were run.

To confirm that the database has sufficient disk space remaining

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.
2. In the left pane, click Tasks and Information, System Information, and then double-click Database Status. The Database Status window appears.
3. For the first tablespace listed, confirm that the free space is greater than 10 MB.
4. In a terminal window or a command window, navigate to the location of the first tablespace.
5. Enter the `ls -l` command to list the files in the datafile.
6. Look for any files that are approaching 32 GB.
   - If the tablespace has more than one datafile, repeat steps 8 and 9 for each datafile.
   - If the tablespace has one datafile and the size is almost 32 GB, you should add a datafile to the tablespace. (If the tablespace has more than one datafile and the size of all datafiles is nearly 32 GB, you should add another datafile.) However, do not add a datafile if the amount of free space in the datafile is more than 2 GB, as reported in the Database Status window.
   - If the datafile is less than 32 GB and is on a device without room for growth, reclaim disk space. If necessary, move the datafile to a device that can accommodate growth.

   **Important!** You cannot move the SYSTEM, NH_ROLLBACK, and NH_TEMP tablespaces.
7. Repeat Steps 7-10 for each tablespace.
Scan Log Files for Errors

By checking your log files daily or weekly, you can resolve problems before they impact eHealth reports and normal operations. All eHealth system logs are saved in the eHealth/log directory with file names that associate the log file with a system job. Carefully examine the statistics_rollup job log for errors. If the statistics rollup job contains errors, the database could grow much faster than expected which can cause disk space problems and other database issues.

Using OneClick for eHealth, you can quickly find failed jobs by selecting Job History and then sorting by Status. If you want to look at the related log file, note the job type and failure date and time, and then select the name of the system to view the Status Summary window. In the Log Information area, click eHealth Logs. All log files are sorted alphabetically by name.

If you have direct access or can telnet to the eHealth system, you can search multiple logs simultaneously by changing to the eHealth/log directory and entering the following command:

```
grep -i keyword *
```

You can substitute any of the following for keyword: "error", "warning", and "failed". If you are searching in report logs, substitute "no data" for keyword.

Factors that Drive Database Growth

The primary factors that drive database growth vary for the eHealth system types. For standard eHealth systems (as well as Distributed eHealth Systems), the following factors are significant:

- Number of polled elements
- Frequency of statistics data rollup
- Number of analyzed data streams

For Traffic Accountant systems, the following factors are significant:

- Number of unique combinations of conversations data
- Frequency of conversations data rollup

Before you change these factors, resize your database accurately using the eHealth Sizing Wizard.

How Polled Elements Impact Database Growth

With each poll, eHealth saves performance data for each element. The eHealth database has to have enough disk space to accommodate the number of elements in your database.
The number of elements that you monitor can grow over time as you add more resources. If you double the number of polled statistics elements, the database doubles its disk space requirements. For example, if you originally planned to add 10,000 elements to your database, and your system grows to 20,000, your database requirements will grow from 33 GB to 66 GB.

Not all elements consume disk space, however. For example, eHealth does not save data for the interface subcomponents of routers. Instead, it aggregates the data to the parent element. When you use the eHealth Sizing Wizard, count the number of elements that consume at least one poller license.

How the Statistics Data Rollup Impacts Database Growth

To minimize the amount of disk space that the database uses for statistics data, eHealth rolls up the five-minute as-polled samples into hourly and daily samples for a specified number of weeks. When data ages beyond the last sample, eHealth removes it from the database.

By default, eHealth keeps the last three days of as-polled (or raw) data. It then does the following:

1. Rolls up the as-polled data into hourly samples.
2. Retains those hourly samples for six weeks.
3. Rolls up hourly samples into daily samples.
4. Retains those daily samples for 70 weeks.

If you need reports that show granular data for longer than three days, you can increase the amount of time that eHealth retains as-polled data by changing the rollup schedule. However, this can substantially increase the size of your database. For example, if you increase the number of days of as-polled data from three days to seven days, you can expect the size of the database to increase by 25%. If you increase the number to 30 days, it will triple the amount of disk space that you need.

To allow for quarter-over-quarter or year-over-year comparisons, you can extend the amount of time that you retain daily samples. If you retain daily samples for two years, the database will typically grow by 15%.

If you modify the default rollup schedule, follow these guidelines:

- Before you change the rollup schedule for as-polled data, use the eHealth Sizing Wizard to estimate the disk space needs and compare them with your current disk space.
- You can decrease the default number of daily samples (70 weeks), but you should keep at least 52 weeks for trend and historical analysis of the performance for the past 12 months.
- After making modifications, check the Database Status window in the OneClick for eHealth console every day for a few days to confirm that the database is growing at the rate that you expect.
How Analyzed Data Streams Impact Database Growth

A scheduled job called Data Analysis runs daily to speed up scheduled Service Level, Health, and MyHealth reports. Data analysis computes values such as health exceptions, service level ranges, and situation-to-watch trends based on performance thresholds defined in service profiles. For each combination of a scheduled report, service profile, and group, eHealth saves a “stream” of analyzed data in the eHealth database. This data enables the report to run much faster than it would if eHealth performed the analysis during report generation.

The following table shows the rates at which disk space increases when you add another scheduled report for the same group of elements using a different service profile. The rate differs based on the number of technology types that you are monitoring with scheduled reports.

<table>
<thead>
<tr>
<th>Number of Technology Types</th>
<th>Additional Disk Space Required Per Additional Scheduled Report Using a Different Service Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 GB</td>
</tr>
<tr>
<td>2</td>
<td>3 GB</td>
</tr>
<tr>
<td>3</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

These estimates are valid for systems monitoring up to three technology types. If you have more than five service profiles and monitor more than five technology types, the additional disk space needed when you add a service profile is significant; use the eHealth Sizing Wizard to plan for the additional disk space.

How Combinations of Conversations Data Impact Database Growth

When you use eHealth Traffic Accountant, the eHealth database saves a record of each conversation observed by an RMON2 probe or data source (such as a Cisco NetFlow collector). Depending upon the number of users in your network, how often they send and receive traffic, and the location of each probe (that is, the LAN/WAN segment in which the probe resides), the database log could show a large number of unique node names and conversations.

The following table shows estimates of database growth when the rate of conversations increases or you increase the number of probes observing the traffic.

<table>
<thead>
<tr>
<th>Rate of Conversations per Minute</th>
<th>1 Probe</th>
<th>2 Probes</th>
<th>3 Probes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>31 GB</td>
<td>33 GB</td>
<td>36 GB</td>
</tr>
<tr>
<td>2,000</td>
<td>33 GB</td>
<td>38 GB</td>
<td>44 GB</td>
</tr>
<tr>
<td>3,000</td>
<td>36 GB</td>
<td>43 GB</td>
<td>51 GB</td>
</tr>
</tbody>
</table>
To minimize the amount of disk space that the database uses for conversations data, eHealth rolls up conversations data. By default, eHealth keeps three days of as-polled (or raw) data. It rolls up the as-polled data into four-hour samples for four days, and rolls up the four-hour samples into daily samples for one week. It also rolls up the daily samples into weekly samples for four weeks. When data ages beyond the last sample, eHealth removes it from the database.

If you need detailed reports for the past week or month, you can increase the amount of time that eHealth retains as-polled data by changing the rollup schedule. However, this will increase the size of your database. For example, if you have three probes and they observe 5,000 conversations per minute, increasing the as-polled conversations data from three to seven days requires 1.5 times the disk space (66 GB to 97 GB). Increasing the as-polled data from three to 30 days will cause your disk space needs to quadruple (66 GB to 279 GB).

If you need to perform quarter-over-quarter or year-over-year comparisons of weekly samples, you can increase the number of weekly samples from 50 weeks to 104 weeks. This change has a minor impact on disk space, adding about 1 GB to your existing database.

### Statistics Rollup Scheduled Job

The statistics rollup scheduled job controls the schedule by which eHealth keeps, aggregates, and deletes the performance data for your elements. By default, eHealth retains as-polled statistics on each element for the previous two days. It then summarizes the as-polled data into hourly samples for the previous several weeks, and into daily samples for the previous several months, as shown in this table.

<table>
<thead>
<tr>
<th>Data</th>
<th>Rollups</th>
</tr>
</thead>
<tbody>
<tr>
<td>As-polled statistics data</td>
<td>2 days</td>
</tr>
<tr>
<td>Hourly samples of statistics data</td>
<td>6 weeks</td>
</tr>
<tr>
<td>Daily samples of statistics data</td>
<td>70 weeks</td>
</tr>
</tbody>
</table>

By default, the statistics rollup job runs each night at 8 P.M. This is typically a low-usage time for the eHealth system. However, if users in your environment are running ad-hoc reports or scheduled reports during this time, you should change the job to run at a less busy time of the day.
As a best practice, the statistics rollup job should run after the scheduled reports for that day have completed so that the reports use the latest raw data. Because users schedule reports to run in the early morning hours, it is best to run the rollup job in the evening of that day. If you have to run the rollup job before your daily reports, you should increase the number of as-polled days from two to three. By keeping an extra day of as-polled data, reports such as Health reports can rank elements for the day prior to a daily report for yesterday.

**Important!** Never disable the Statistics rollup job unless directed to do so by Technical Support. If you disable this job, the database will quickly consume the available disk space. If you must disable this job temporarily for any reason, re-enable it as soon as possible.

Typically, you should save at least one year (52 weeks) of daily samples for trend and historical analysis. Daily samples do not consume much disk space. For example, one year of rolled-up daily samples uses as much disk space as a day and a half of as-polled data at a five-minute polling interval.

If you increase the number of days of as-polled data, you may need to create a new database or add more disk space to make sure that the database does not outgrow the partition on which it resides.

**Change the Statistics Rollup Schedule**

You can modify the statistics rollup job by using the OneClick for eHealth console. You can change the day or time at which rollup occurs, change specific job parameters, and specify how long to retain data samples.

**To modify an eHealth scheduled system job**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage scheduled jobs.
2. In the left pane, click Tasks and Information, Job Scheduler, and then double-click Scheduled Jobs.
   The Scheduled Jobs window appears.
3. Select the job that you want to modify, right-click, and select Edit job.
   The Edit Job window appears.
4. Select the Schedule tab; change the day, time or month; and click OK.
   eHealth changes the job schedule accordingly.
5. Select the Properties tab, if applicable, and change the parameters of the job.
   eHealth changes the job accordingly.
Live Exceptions Baseline Scheduled Job

If you use Live Health and have configured it to monitor elements using Deviation From Normal, Time Over Threshold, or Time Over Dynamic Threshold rules, eHealth uses historical data to calculate a baseline for comparison. A baseline is the typical behavior of an element (or group or group list) based on the past several weeks.

By default, the Live Exceptions baseline job runs at 7:00 P.M., and retains the data for six weeks. Each new day, Live Exceptions deletes the oldest day of data. This schedule enables Live Exceptions to retain enough information about historical performance without consuming an ever-increasing amount of disk space.

You can schedule the Live Exceptions baseline job to run at any time of the day, but make sure that you choose a time that allows it to finish running before midnight so that Live Exceptions calculates alarms by using the most current baseline.

**Important!** You should not disable the Live Exceptions baseline job. It immediately affects Time Over Dynamic Threshold alarms. If the job is disabled for a week or longer, it also impacts Deviation From Normal alarm comparisons.

You can increase the number of weeks of Live Exceptions data to include in the baseline period. For example, if your IT environment experiences quarterly trends, you can include 13 weeks of Live Exceptions data in the baseline. This increase has a minimal impact on disk space.

Live Exceptions History Scheduled Job

If you use Live Health, you can view historical alarms in the Live Exceptions Browser. By default, the Live Exceptions History job runs each day at 6:00 P.M and deletes alarm data that is more than two days old.

You can change the job setting to keep alarm data from 1 to 7 days. (eHealth cannot keep alarm data that is more than eight days old.) Also, you can schedule the Live Exceptions history job to run any time of day; running it at different times does not impact eHealth reports or other jobs. Typically, you should not disable the Live Exceptions history job, but you can modify it by using the OneClick for eHealth console.

Delete Database Archive Logs Scheduled Job

Archive logs are backup copies of filled redo logs that provide the capability to recover to a specific point in time for any tablespace in the database. Archive logs consume disk resources; they can also cause the database to freeze if the disk on which the archive logs reside is filled.
To prevent this from occurring, eHealth regularly deletes archive logs from the system.

- If you are using a full backup strategy, the Delete Database Archive Logs job deletes archive logs on an hourly basis. You cannot modify or disable this job.
- If you are using an incremental backup strategy, the Delete Database Archive Logs job is disabled so that the logs can be used for point-in-time recovery of the database. eHealth regularly deletes old archive logs after each level 1 save.

The Delete Database Archive Log job saves information about the job in the following file:

```
/eHealth/log/Delete_Database_Archive_Logs.jobId.log
```

**Database Maintenance Scheduled Job**

The Database Maintenance job performs several maintenance operations on tablespaces and indexes to enable the database to use existing space effectively. This scheduled job runs every Sunday at 10:30 A.M. If you disable this job, your database could grow more quickly than expected. The Maintenance log saves information about the job in the `/eHealth/log/DB_Maintenance.100015.log` file.

**Delete Temporary Tables Scheduled Job**

The Delete Temporary Tables job deletes temporary tables that are more than four hours old if they are no longer in use. This job runs every four hours automatically. If you disable this job, your database disks could fill up if a process creates a large temporary table and exits abnormally.

**Delete Old Reports Scheduled Job**

To maintain disk space in the eHealth home directory, eHealth automatically runs the Delete Old Reports job at 6:00 A.M. daily. This job deletes temporary files that are more than four days old, and it removes saved reports that are more than 31 days old.

**To modify the Delete Old Reports scheduled job**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage scheduled jobs.
2. In the left pane of the console, click Tasks and Information, Job Scheduler, and then double-click Scheduled Jobs. The Scheduled Jobs window appears.
3. Select the Delete Old Reports job from the job list, right-click, and select Edit Job. The Edit Delete Old Reports window appears.
4. Do the following, and then click OK:
   a. Select the Properties tab and change the number of days to retain report files. (For Health and Service Level reports, you can change the number of days to retain daily, weekly, and/or monthly report files.) Also, change the number of days to retain temporary files saved in the eHealth/tmp directory.
   b. Select the Schedule tab and specify a daily or monthly schedule and the time when the job should run.
      eHealth changes the job schedule accordingly.

Conversations Rollup Scheduled Job

Traffic Accountant is an eHealth application that enables you to discover and poll probes, and to generate three types of Traffic Accountant reports to analyze data that is sent between nodes in your IT infrastructure. The Conversations Rollup scheduled job controls how eHealth keeps, aggregates, and deletes the performance data for your Traffic Accountant (TA) elements. By default, it runs each night at 12:05 P.M. and repeats every four hours during the day.

EHealth rolls up two sets of conversations data: all conversations and top conversations.
   - All conversations data is every conversation reported by every probe element. The database might have several entries for a conversation if more than one probe reported it.
   - Top conversations data is a single entry for every conversation, based on what eHealth calculates as the best data for that conversation.

EHealth maintains a separate rollup schedule for each set of conversations data. In general, you may want to retain more of the top conversations data when your reports focus on the overall conversations that occurred within the network. You may want to retain more of the all conversations data when your reports focus on the traffic observed by each probe.

**Important!** Use caution when specifying the number of days and weeks to keep data, particularly as-poll data. You can decrease the default number of daily samples (70 weeks), but you should keep at least 52 weeks for trend and historical analysis of the past year’s performance. Never disable the conversations rollup job unless directed to do so by Technical Support. If you turn off the job, your database will quickly consume available disk space.

For instructions on modifying the conversations rollup schedule, see the eHealth Traffic Accountant and Cisco NetFlow Administration Guide.

Cleanup Nodes Scheduled Job

To conserve disk space in the database, eHealth can hide or delete records for nodes or autonomous systems that have not been referenced for a specified time period. (An autonomous system is a collection of networks under a common administration that share a routing strategy.) When records for nodes or
autonomous systems are hidden, you can run reports on their data. However, eHealth removes records of hidden nodes or autonomous systems once it rolls data out of the database. If a probe observes traffic for nodes or autonomous systems with records that have been hidden, the nodes or autonomous systems then reappear in subject lists so that you can run reports on them.

eHealth can also permanently remove records of nodes or autonomous systems when they have not been observed for a specified time period. This setting is useful when you suspect that those nodes or autonomous systems were transient and are not likely to be observed again, and you do not plan to run reports for that data.

**FSA Scrubber Scheduled Job**

If you have a Distributed eHealth System, it runs the File Staging Area (FSA) Scrubber job every four hours to remove temporary files in the FSA and soft-deleted objects that still have entries in the database. An object can be a group, service profile, or group list. You should not modify this job. For more information on the Distributed eHealth scheduled system jobs, see the *Distributed eHealth Administration Guide*.

**eHealth Database Backups**

The standard eHealth database save utility performs a full binary save using Oracle’s Recovery Manager (RMAN). The full database save is platform-dependent, path-dependent, and language-dependent:

- **Platform-dependent** – Full database saves are platform-dependent, but not system-dependent. That is, you cannot save a database on a Windows system and then load it onto a Solaris system, but you can load a database saved on one Solaris system to another Solaris system.

- **Path-dependent** – eHealth remembers the path to which a save was performed. When you attempt to load the files, eHealth attempts to find the files to load only in the directory in which they were saved.

- **Language-dependent** – You can load an English database onto an English system only, and you can load a Japanese database onto a Japanese system only.

You can back up your database using one of the following methods:

- **Standard (Binary) Save** – A standard save is a full database backup saved as binary data. Standard saves can be loaded onto any eHealth system of the same platform type, but the location of the datafiles is path-dependent; that is, the location of the datafiles for both the new machine’s database and the saved database must be exactly the same. Perform a standard save when you want an immediate (non-scheduled) backup of your system, such as before installing an eHealth upgrade, or when you want to move the database to a new eHealth system.
- **Incremental Save** – Incremental save is an improved eHealth backup strategy available in this release. Incremental saves consist of two separate types of saves:
  - **Level 0 Save** – A Level 0 save is a full database backup, similar to a full (standard) save. It takes about the same amount of time and disk space as a full save. You generally schedule Level 0 saves to occur weekly in an incremental save strategy.
  - **Level 1 Save** – A Level 1 save does not save a full copy of the database; instead, it saves only the data blocks that have changed since the previous backup. This saves both time and disk space. You generally schedule Level 1 saves to occur daily in an incremental save strategy.
  
  The speed and flexibility of incremental saves make them a powerful tool for regular database backups. To protect your eHealth data, you should schedule incremental saves to back up your database daily.

- **Universal (ASCII) Save** – A universal save is a full database backup that is platform-independent, path-independent, and language-independent. Universal saves are smaller and more flexible than binary saves, but take longer to restore than binary saves. Perform a Universal Save when you want to move the database to an eHealth system of a different platform type.

Important! You must back up your eHealth database using one of these methods. Do not use Oracle backup tools or backup tools provided by another vendor. Never use third-party software or the Oracle backup tools to back up the eHealth database. Backing up database files using third-party software may corrupt the database by interfering with the internal locking mechanisms used by Oracle. If you use third-party backup software, make sure that you exclude the database files. To back up the eHealth database, use database save procedures. Once the database save has finished, you can back up the archive using your third-party backup software.

**Incremental Saves**

Incremental Save is a database backup strategy consisting of two separate types of saves, level 0 and level 1. Using incremental saves, eHealth does not save a full copy of the database each day; instead, it saves the full database once each week (level 0) and saves only the changes that occur daily (level 1). This strategy saves both time and disk space, and allows greater flexibility for backup and recovery.

The weekly level 0 save is similar to a full database save and consumes about as much time and disk space. However, each level 1 save consumes less time and disk space because eHealth saves only the data blocks that have changed, freeing the system to perform other database-intensive tasks. Incremental saves allow you to recover the database to the time of the last level 1 or level 0 save.

Important! Every time that you perform a level 0 save, you overwrite the last full save. To make sure that you always have a good backup from which to restore your database, perform at least two full saves before performing a level 0 incremental save.
A daily level 1 save consumes less time to complete than a full database save. Incremental saves can also write data to multiple locations at once, allowing faster completion of both level 0 and level 1 saves. You can schedule level 1 saves to occur several times a day, minimizing any data loss to a few hours. Because an incremental save records a history of all database changes, you can easily restore the database to the point of the last level 1 save, or to the point of any subsequent level 0 save. eHealth performs several diagnostics so that the saved database is valid for recovery. If a save does not pass the diagnostic tests, eHealth retains the previous save.

**Note:** When you receive a trap from a SystemEDGE agent, the incremental save fails.

**Universal (ASCII) Saves**

A universal save (also called an ASCII save) is a full database save that you can load onto an eHealth system of any platform type. For example, using a universal save, you can save an eHealth database on a UNIX system and then load it into an eHealth database that is running on a Windows system.

The universal save writes data in an Oracle-proprietary, platform-independent, binary format. To load your database into an eHealth database that is running on a different platform, you must use this option when you save the database. Universal saves are also path-independent, which means that you can save them to any directory and load them to a different directory on the same system or another system.

The universal save is also language-independent, which means that you can load an English database onto a French, Spanish, or Japanese system, a French or Spanish database onto an English system, and so on. You cannot, however, load a Japanese database onto an English, French, or Spanish system because those systems do not support double-byte characters.

Although universal saves are smaller and more flexible than binary saves, they take much longer to restore than binary saves. Universal saves can also be loaded into a system that has a different Oracle SID and a different eHealth user from the one in which you saved the database.

**How Database Saves Work**

eHealth database saves occur while the eHealth server is online. eHealth continues to poll elements and process scheduled jobs while the database save runs. When you save your eHealth database, you and your users do not experience data loss or downtime. However, to minimize performance impacts to other scheduled jobs or ad-hoc reports, you should schedule backups to run and finish during time periods of low usage.

Because the database remains online during backups, any changes to the database that occur while the save is in progress are collected in archive logs. When you load a saved database, the nhLoadDb utility makes the database files consistent by applying the archive logs. eHealth does not use archive logs when loading a universal (ASCII) save.
When you perform a full save (standard, universal, or incremental level 0),
eHealth essentially unloads the entire database and saves it to a set of files,
similar to a data-export. eHealth saves all of the tables in the system, one at a
time, and copies the data from each table to this set of binary or ASCII files. It
then compresses these files into an archive and stores them in the destination
directory.

Along with the database, eHealth also saves the following report and
configuration files:

- Object model extension (.omx) files
- Report (.rpt, .dac, .rds, .rde, .sds, .sde, .vpns, and .mhd) files
- Report presentation variable (.vars) files
- Database data information (.ddi) files
- Database layout configuration (.lcf) files
- Time zone information
- Traffic Accountant view definitions

When you perform an incremental level 1 save, eHealth does not save the entire
database; instead, it analyzes each of the tables in the system, and copies the
changed data blocks to a set of binary files. It then compresses these files into
an archive and stores them in the destination directory.

**Disk Space Requirements**

When choosing locations for your backups, make sure that they combine to
provide adequate disk space. The following table provides estimates of the size
of a standard save based on the number of polled elements and the number of
days of as-polled data.

<table>
<thead>
<tr>
<th>Number of Elements</th>
<th>7 Days of As-Polled Data</th>
<th>30 Days of As-Polled Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>6 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>10,000</td>
<td>10 GB</td>
<td>21 GB</td>
</tr>
<tr>
<td>25,000</td>
<td>22 GB</td>
<td>51 GB</td>
</tr>
<tr>
<td>40,000</td>
<td>32 GB</td>
<td>77 GB</td>
</tr>
</tbody>
</table>

When you schedule standard saves (or if you perform a standard save to the
same location as an existing save), eHealth retains each existing save until the
new save finishes and it validates it. Therefore, you must have adequate disk
space for at least two full saves. For example, if you poll 10,000 elements and
save 30 days of as-polled data, you should choose backup locations that have at
least 42 GB (2 x 21 GB) of disk space.
The space requirements for an incremental level 0 save and a standard database save are roughly the same. However, the space required for level 1 saves can be difficult to estimate since it depends on the magnitude of changes to the database each day. A rough estimate of disk space required for a level 0 save and six level 1 saves is three times the size of a level 0 save.

**Best Practices for Performing Database Saves**

When performing a database save, follow these guidelines:

- Always perform backups using the eHealth database save commands to make sure that you can easily restore the saved database.
- Do **not** use Oracle tools or other third-party software to back up database files. Doing so can corrupt the database.
- Make sure that the locations to which you are saving the database have sufficient disk space for the backup. If you specify multiple locations, eHealth splits the backup data equally over the locations that you specify. It does not consider available disk space.
- Do not save the database to an NFS-mounted disk or mapped drive. eHealth **does not** support database saves to NFS-mounted disks or mapped drives.
- On Windows systems, do **not** include accented characters in pathnames or file names. If you use accented characters, the load utility cannot identify the location and cannot load the database.
- Do not use the UNIX tape archive (tar) utility on files that are larger than 2 GB. For larger files, you must split the saved files and tar the resulting smaller files.
- When performing an incremental save, always review the `rman_save*.log` file (located in the `ehealth/oracle_rman` directory) to confirm that the backup is still running.
- eHealth deletes the previous full save (standard or level 0) after you perform a new full save. Therefore, you should **always** archive each full save by copying it to another disk or using a third-party backup utility. This strategy enables you to restore the database to the last good day, even if corruption occurred gradually.

**Perform a Full Database Save**

You can use the eHealth standard database save utility to perform an immediate backup of the eHealth database. The full database save is not a substitute for regularly scheduled backups, but it is useful when you want to save your database manually.

You should perform a full database save at the following times:

- Before upgrading eHealth
- Before upgrading Oracle
- Before loading previously saved data into your database
- Before moving the database
- After you add new datafiles or move existing datafiles
Saving a large database with a standard save takes approximately one hour. If you perform a full save to the same location as an existing save, eHealth retains the existing save until the new save finishes successfully. After eHealth validates the new save, it deletes the prior save.

**To perform a full database save from the eHealth console**

1. Select Database, Save Database.
2. In the Save Database As field of the Save Database dialog, specify the directory in which to save the database.
3. Click Save.

   eHealth saves the database to the specified location. Depending on the size of your database, the save can take up to one hour.

   You can also perform a full database save using the nhSaveDb command. This command allows you to select multiple locations for the save, which may allow the backup to finish in less time. For more information, see the *eHealth Commands and Environment Variables Reference Guide*.

**Best Practices for Database Backups**

You need to develop an effective backup strategy so that you can recover your eHealth system quickly in the event of a disk failure, database corruption, or other unexpected event. Without a backup strategy, you may need to spend hours or days reinstalling and reconfiguring eHealth, and could lose valuable data.

To prevent data loss, you should save your database on a *daily basis*. As a best practice, follow these guidelines:

- Perform at least two full saves (before a level 0 incremental save) to prevent the new save job from overwriting the old one so that you will always have a good backup from which to restore your database.
- If you are running the current release of eHealth, use the incremental save feature to schedule a full database save (level 0 save) once each week, and use daily level 1 saves to capture daily database changes. This strategy saves both time and disk space (compared to daily standard saves), and allows greater flexibility for backup and recovery.
- If you need maximum protection from potential data loss, schedule level 1 incremental saves to occur several times each day. This strategy requires more disk space, but prevents you from losing more than a few hours of historical data.
- If you are running an eHealth release earlier than r6.1, schedule a standard (binary) database save to occur once each day during a period of low database activity.
- Always archive several months of database saves, and keep the archives in a different physical location from the database disks. This strategy protects the integrity of your backups, and allows you to restore the database to the last good day, even if corruption occurred gradually.
- Perform periodic universal (ASCII) saves in addition to your regularly scheduled standard saves. You would load the ASCII save only if your binary saves are corrupted or otherwise cannot be restored.
- Always perform backups by using the eHealth database save commands to make sure that you can easily restore the saved database.
- Do not save the database to an NFS-mounted disk or mapped drive. eHealth does not support database saves to NFS-mounted disks or mapped drives.

**Schedule Incremental Saves**

If you schedule regular database backups, you can restore your data in the event of a system failure. If you are running the latest release of eHealth, you should schedule incremental saves to back up your database.

**Important!** You cannot use the Schedule Jobs dialog to schedule incremental saves, and you cannot schedule an incremental save if a full backup has been scheduled.

**To schedule incremental saves**

1. Determine the best time to perform saves. Saves take place while the eHealth server is online, so data loss or downtime does not occur. However, since saves consume system resources, you should schedule backups for a period of low usage to minimize performance impacts to other scheduled jobs or ad-hoc reports.
2. Determine the disk locations in which you want to save the backup. Using more than one location enables the backup to finish in less time. You may choose up to 10 locations. Enter the following command:

   ```
   nhSaveDbConfig
   -add -incrLevel0Days 7
   -incrLevel1 daily yyyyyyy
   -startDate MM/DD/YYYY
   -startTime HH:MM
   -p first_save_location/backup.tdb
   -p second_save_location/backup.tdb
   ```

   where:
   - `-startDate` specifies the date of the first level 0 save. If the NH_DATE_FMT environment variable is set to DMY, you must use the DMY format for the start date.
   - `-startTime` specifies the time that the level 0 or level 1 backup starts each day.
   - `-p` specifies each of the paths in which the backup data is saved.

For a complete description of the nhSaveDbConfig command, see the *eHealth Commands and Environment Variables Reference Guide*. 
For example, the following command schedules an incremental level 0 save to occur every Sunday at 11:15 P.M. and schedules a level 1 save to occur Monday through Saturday at the same time. The data from the backup is split evenly over two locations (diskFarm10 and diskFarm12).

```
nhSaveDbConfig  
    -add -incrLevel0Days 7  
    -incrLevel1 daily nyyyyyy  
    -startDate 07/16/2006  
    -startTime 23:15  
    -p /export/diskFarm10/eHealth/incBackup2.tdb  
    -p /export/diskFarm12/eHealth/incBackup2.tdb
```

eHealth automatically disables the Delete Database Archive Logs scheduled job when you schedule incremental saves because those logs are utilized for point-in-time recovery. Archive logs provide the capability to recover to a specific point in time for any tablespace in the database.

**Modify a Incremental Save Scheduled Job**

Each eHealth system can support only one incremental save job. Therefore, to change the schedule when saves occur, or to add or change the paths of an existing scheduled save, you must delete the job and then schedule a new incremental save job.

**To modify a scheduled incremental save**

1. In a command window, log in as the eHealth user and enter the following command to identify the job ID of the incremental save job:

   ```
nhSaveDbConfig -list
   ```

   The command lists each type of backup that you have scheduled by using the nhSaveDbConfig command. Assume that the job has a job_ID of 1.

2. Enter the following command to delete the job_ID 1:

   ```
nhSaveDbConfig -delete 1
   ```

3. Schedule a new save by running the nhSaveDbConfig command.

**Delete a Incremental Save Scheduled Job**

You cannot modify an existing scheduled save. If you want to change the time at which a save occurs, or the paths to which data is saved, you must delete the job and then schedule a new incremental save.
To delete an incremental save job

1. In a command window, log in as the eHealth user and enter the following command to identify the job ID of the incremental save job:
   
   \texttt{nhSaveDbConfig -list}
   
   The command lists each type of backup that you have scheduled using the \texttt{nhSaveDbConfig} command. For this example, assume that the incremental save job has a job ID of 1.

2. Enter the following command to delete the job ID 1:
   
   \texttt{nhSaveDbConfig -delete 1}

3. Schedule a new incremental save with the appropriate parameters.
   
   **Important!** Each eHealth system can support only one incremental save job.

Schedule Full Database Saves

If you are using an earlier eHealth release, you should schedule a full database save to occur daily during a period of low database activity. Any database that you restore contains only the data that was current when you last saved the database, so it is important to have a recent backup available.

With the latest eHealth release, some small environments (with less than 3,000 elements) may choose to continue using a daily full database save to back up their database. However, you should consider using the incremental save strategy because of the greater flexibility for backups and point-in-time recovery.

eHealth does not create a backup copy of an existing database save. It retains each one only until the next save finishes successfully. After it validates the new save, it deletes the previous save. For full coverage, you should always archive each backup after the save finishes.

To schedule a database backup

1. Select Setup, Schedule Jobs on the console.
   
   The Schedule Jobs dialog appears.

2. Select Add Db Save from the list of default jobs.
   
   The Add Scheduled Database Save dialog appears.

3. Do the following:
   
   a. Under Save Database As, specify a name for the directory in which to save the database.
   b. Under Schedule, select on these days and select the days on which the backup occurs.
   c. Specify the time at which the database backup should begin.
**Important!** Backups do not cause system downtime, but you should schedule backups for a period of low database usage to minimize performance impacts on other scheduled jobs or ad-hoc reports.

4. Click OK in the Schedule Jobs dialog.

If you use the nhSchedule command to schedule backups, you can select multiple paths for your saves, which may allow the backups to finish in less time. For more information, see the *eHealth Commands and Environment Variables Reference Guide*.

**Monitor Disk Space Available for Backups**

It is important to monitor your disk space because a full disk can cause a save to fail. After you schedule database backups, you should use a system management agent such as the Unicenter NSM agent or the eHealth SystemEDGE agent to monitor the space on the disk on which the backups reside. The agent can notify you when disk usage reaches a certain threshold so that you can take steps to acquire more disk space.

In addition, when you initially set up an incremental save strategy, you should monitor how much space your level 0 and level 1 saves require. This information is valuable if you consider changing the frequency of incremental saves or the backup locations. If you recently installed eHealth, the initial saves will be smaller and grow over time as the database fills with as-polled and rolled-up data. For example, if eHealth saves 30 days of as-polled data, the database will not be full for 30 days. To manage the size of backups, you can specify the -listSizes argument with the nhSaveDbConfig command to display the amount of disk space used by each scheduled save. The following is a sample of the command output:

```
| Backup | Func | Total | Full | Incremental | Files Only | Last Good Backup | Last Bad Backup |
|--------|------|-------|------|-------------|------------|------------------|----------------|----------------|
| ASCII  | MAX  | 22107 | 4851 | 0           | 17256      | 08/09/2005 09:41:18 |
| ASCII  | AVERAGE | 22004 | 4748 | 0           | 17256      |
| ASCII  | LAST | 22107 | 4851 | 0           | 17256      | -                |
| FULL   | MAX  | 351092| 333835| 0          | 17257      | 07/25/2005 09:26:41 |
| FULL   | AVERAGE | 351092| 333835| 0          | 17257      |
| FULL   | LAST | 351092| 333835| 0          | 17257      | -                |
| INC0   | MAX  | 348100| 330844| 0          | 17256      | 07/25/2005 09:55:25 |
| INC0   | AVERAGE | 348100| 330844| 0          | 17256      |
| INC0   | LAST | 348100| 330844| 0          | 17256      | -                |
| INC1   | MAX  | 356714| 339458| 8604       | 17256      | 07/25/2005 10:12:19 |
| INC1   | AVERAGE | 356714| 339458| 8604       | 17256      |
| INC1   | LAST | 356714| 339458| 8604       | 17256      | -                |
```

Archive Saves

After you schedule saves, establish procedures for copying the backups to tape or another system that is in a directory owned by a secure user who has read-only permissions. (Any users who have access to the saved database can restore it on another system and view all of the data that it contains.) For maximum recovery safety, the archived data should be moved offsite. You might also find it valuable to invest in a remote storage solution like BrightStor that makes the management of tape libraries obsolete.

You should retain several months of archived backups so that you can flexibly recover eHealth data and reports. This also enables you to recover most of your data if a corruption occurred undetected over time.

How to Recover the Database from a Backup

An incremental save strategy provides you with several options for restoring your eHealth database in the event of a failure. If a disk failure or other hardware issue causes you to lose data, you can recover the database to the point of the last backup. If data corruption occurred gradually, you can revert the database to a point prior to the corruption.

In the event of a disk failure, database corruption, or other unexpected event that causes data loss, you can restore your database from a backup. Depending on the backup strategy you have implemented, you can do one of the following:

- Perform a recovery to the previous time of a level 1 or level 0 save (Incremental Saves Only).
- Perform a partial recovery of specific parts of the database (Incremental Saves Only).
- Restore the database from a previously saved full backup.

Follow these guidelines:

- Make sure that the eHealth system on which you load a database is at the same release or later than the system on which the database was saved.
- Make sure that the system onto which you are loading the database has enough free disk space to support the database. If a disk does not contain enough space, eHealth displays an error message that identifies the disk, the amount of space that it is lacking, and the files on that disk. You can then add another datafile to the tablespaces on that disk, or you can move one of the tablespaces to another disk that has more space.
- Make sure that the number of files in each tablespace in the saved database is less than or equal to the number of files in each tablespace in the database in which you to load the saved data.
- On Windows systems, make sure that the pathnames and file names of the saved database do not include accented characters. If the path names contain accented characters, the load utility cannot identify the location and cannot load the database.
If a database load fails, recreate the database using the nhDestroyDb and nhCreateDb commands, and then reload the backup. For more information on these commands, see the eHealth Commands and Environment Variables Reference Guide.

If a database load is interrupted before it finishes, restart the load procedure. If the second load fails, recreate the database using the nhDestroyDb and nhCreateDb commands.

When loading a standard (binary) database save, eHealth recreates the database password file and resets database passwords to eHealth for all accounts. After you load a database, always change the database passwords for eHealth administrator-level accounts using the nhManageUsers command.

Perform Full Recovery from an Incremental Backup

If a disk containing part of the database fails, a database file is accidentally deleted, or you lose your eHealth system due to a natural disaster or other unexpected event, you need to restore the database to its most recent state by performing a full recovery.

To perform a full recovery

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:
   
   `nhServer stop`
3. Enter the following command to load the database:
   
   `nhLoadDb -p path1 -defaultRecovery`
   
   where `-p` specifies the first path in which the backup data is saved (see Schedule Incremental Saves on page 128). You only need to specify the first path when loading the database.
   
   **Note:** For a complete description of the nhLoadDb command, see the eHealth Commands and Environment Variables Reference Guide.

   For example, the following command restores the database to its state immediately prior to the time a disk failed.

   `nhLoadDb -p /export/diskFarm10/eHealth/incBackup2.tdb -defaultRecovery`
4. After the load finishes, restart the eHealth server by entering the following command:
   
   `nhServer start`
5. Monitor the polling status windows to verify that the poller is running.
6. Examine the database status to verify that the database loaded successfully.
7. Using the nhManageUsers command, change the database passwords for all eHealth administrator-level accounts.

   During the database load, eHealth recreates the database password file and resets database passwords to eHealth for all accounts. After you load a database, always use the nhManageUsers command to change the database passwords for eHealth administrator-level accounts.
Perform Point-in-Time Recovery from an Incremental Backup

If a software failure corrupts data in the database, you need to recover the database to a point in time before the data corruption occurred. This action is called a point-in-time recovery. Using point-in-time recovery, you can recover your database to the time of the last full (level 0) backup, or to the time of any subsequent level 1 backup. For example, if you determine that corruption took place on Wednesday at 1:15 P.M., and a level 1 backup occurred at 12:00 P.M. that day, you could restore the database to its state as of 12:00 P.M., prior to the point of corruption.

Before you perform a point-in-time recovery, you must determine the approximate time that data corruption occurred so that you can restore the database to a time before the corruption.

To perform a point-in-time recovery

1. Enter the following command to identify times for which recovery is available:
   
   ```
   nhLoadDb -showRecoveryTimeRange -p path
   ```

   eHealth displays the time range within which recovery is possible.

2. Determine the time at which the data corruption occurred. If corruption occurred after any of the times listed, you can perform a point-in-time recovery. If not, you may need to perform a partial recovery of a previously archived backup. See Perform Partial Recovery from an Incremental Backup on page 136.

3. Enter the following command to stop the eHealth server:
   
   ```
   nhServer stop
   ```

4. Enter the following command to load the database:
   
   ```
   ```

   where:
   
   - `-p` specifies the first path in which the backup data is saved. You only need to specify the first path.
   - `-pointInTimeRecovery` specifies the date and time on which you want to restore the database.

   **Note:** For a complete description of the `nhLoadDb` command, see the eHealth Commands and Environment Variables Reference Guide.

   For example, the following command would restore the database to 3:25 P.M. on July 14, 2006.

   ```
   nhLoadDb -p /export/diskFarm10/eHealth/incBackup2.tdb -pointInTimeRecovery 07:14:2006:15:25:00
   ```

5. After the load finishes, restart the eHealth server by entering the following command:
   
   ```
   nhServer start
   ```

6. Monitor the polling status windows to verify that the poller is running.
7. Examine the database status to verify that the database loaded successfully.
8. Use the nhManageUsers command to change the database passwords for all eHealth administrator-level accounts.

Recover the Database from a Standard Backup

If you are using a standard backup strategy, you can restore the database to the point at which the last standard backup occurred. When you load the backup, eHealth completely replaces the contents of the current database with the saved database.

The saved database files must be located in a directory that has a .tdb extension and is writable. In addition, if you are loading the database onto a different system (such as a backup server), the following restrictions apply:

- The systems must be of the same platform type.
- The path to which the database was saved must be identical to the path from which you are loading it.
- NH_USER and Oracle SID must be the same.
- The number of files per tablespace must match on the save and load systems.

Important! If your current database is corrupt, you must recreate the database using the nhDestroyDb and nhCreateDb commands before loading the backup. For more information on these commands, see the eHealth Commands and Environment Variables Reference Guide.

To recover the database from a full backup

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:
   ```
   nhServer stop
   ```
   The eHealth server stops.
3. Select Database, Load Database on the console.
   The Load Database dialog appears.
4. Specify a directory in the Load Database From field.
   eHealth automatically appends the .tdb extension to the directory name.
   Important! If you are loading a database onto a Windows system, make sure that the directory and file name for the saved database do not include accented characters. If they do, you must rename them with non-accented characters before the load can proceed.
5. Click Load.
   eHealth performs a standard database load.
6. After the load finishes, select Console, Start Server.
7. Monitor the polling status windows to verify that the poller is running.
8. Examine the database status to verify that the database loaded successfully.
9. Change the database passwords for all eHealth administrator-level accounts using the nhManageUsers command.

During the database load, eHealth recreates the database password file and resets database passwords to eHealth for all accounts.

**Important!** After you load a database, *always* use the nhManageUsers command to change the database passwords for eHealth administrator-level accounts.

You can also perform a database recovery from the command line using the nhLoadDb command. For more information, see the *eHealth Commands and Environment Variables Reference Guide*.

### Perform Partial Recovery from an Incremental Backup

If you are using an incremental backup strategy, you can perform a partial database recovery to recover specific parts of the database that have failed. Using this feature, you can recover a single tablespace, datafile, or corrupt block. Partial database recoveries always recover to the current point in time, so the recovered portion of the database can be made consistent with the rest of the database. For information on performing a partial database recovery, contact Technical Support.

### Recover Element Configuration (without a Backup)

eHealth runs a scheduled system job called Element Configuration Backup whenever it creates a new database or upgrades the database from a previous version, but this job does not appear in the Scheduled Job dialog. This job runs every 4 hours by default and creates a backup of the configuration in a file called elementCfgBackup.dci within the `eHealth/poller` directory. If you lose your database, and you do not have a saved database backup, contact Technical Support for assistance in using this file to recreate the element configuration.

### Move the Database to Another System of the Same Platform Type

If you are upgrading your system to increase disk space, or want to copy the database to a non-production server, you can use the standard full save feature to move the database.

When moving your database to another system of the same platform type, the following restrictions apply:

- The path to which the database was saved must be identical to the path from which you are loading it.
- NH_USER and Oracle SID must be the same.
- The number of files per tablespace must match on the save and load systems.
If you move the database to another system, that system must be running the same (or a later) release of eHealth as the system on which the database currently resides. You can move your eHealth database to a different platform using a universal save and load. For more information, see Move the Database across Platforms on page 138.

**To move your database**

1. Determine the amount of space currently used by the database. Run the nhDbStatus command or select Database, Status from the console.
2. If you plan to move the database to another system, include the total space currently used by eHealth.
3. Select a new location for the database. Verify the name and the available disk space of the new location by entering the command listed in this table.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>df -ak</td>
</tr>
<tr>
<td>HP-UX</td>
<td>bdf</td>
</tr>
<tr>
<td>Windows</td>
<td>dir/s</td>
</tr>
</tbody>
</table>

On a Solaris or HP-UX system, the command displays the available disk space for all mounted disks.

4. Save a copy of the current database.
5. On the new server, enter the following command to stop the eHealth server:
   ```
   nhServer stop
   ``
   The eHealth server stops.
6. Select Database, Load Database on the console.
   The Load Database dialog appears.
7. Specify the directory containing the saved database.
   **Important!** If you are loading a database onto a Windows system, make sure that the directory and file name for the saved database do not include accented characters. If they do, you must rename them with non-accented characters before the load can proceed.
8. Click Load. eHealth begins a standard database load.
9. eHealth checks the system on which you are performing the load to make sure that it has sufficient space and that the number of files per tablespace is sufficient for the loaded database.
   - If the system has sufficient space, eHealth loads the saved files into the new database.
   - If a disk does not contain enough space, eHealth displays an error message that identifies the disk, the amount of space it is lacking, and the files on that disk. If this occurs, add another datafile to the tablespaces on that disk, or move one of the tablespaces to another disk that has more space.
10. After the load finishes, select Console, Start Server.
11. Monitor the polling status windows to verify that the poller is running.
12. Examine the database status to verify that the database loaded successfully.
13. Run the nhManageUsers command to change the database passwords for all eHealth administrator-level accounts.

**Move the Database across Platforms**

You can use a *universal* save and load to move your eHealth database to another platform. For example, you could save an eHealth database on a UNIX system, and then load it into an eHealth database that is running on a Windows system.

Universal saves are also *path-independent*; therefore, you can save them to any directory and load them to a different directory on the same system or another system. They are also *language-independent*, which means that you can load an English database onto a French, Spanish, or Japanese system. You *cannot*, however, load a Japanese database onto an English, French, or Spanish system.

When you save a database using the universal save method, you can load it into a system that has a *different* Oracle SID and a different eHealth user from the one in which you saved the database.

When you are performing universal saves, follow these guidelines:

- If you encounter errors during a universal save, see the `eHealth/log/save.log` and `save_dir.tbd/oracle_export/exp.log` files.
- Universal saves consume more disk space than full (standard) saves. You can, however, compress universal saves considerably (for example, to a compression ratio of four times or more).
- The time to perform a universal load is considerable: it could take up to eight hours to load an extra-large database. Be sure to set aside enough time to perform the load.
- On Windows systems, do *not* include accented characters in directory and file names.

**Note:** If you are unfamiliar with performing universal saves and loads, contact Technical Support before you perform the tasks described in this section.

**To save and load the database across platforms**

1. Create a directory with a .tdb suffix (for example, `/home/myDb.tdb`).
2. Enter the `nhSaveDb` command in a form similar to the following:
   ```bash
   nhSaveDb -p /home/myDb.tdb -ascii
   ```
3. Once you have saved the database, move the files from the directory that you created in Step 1 to a directory on the destination system. The destination directory name must also have a .tdb suffix.
4. At the destination system, stop the eHealth server and use the Load Database dialog or the `nhLoadDb` command to load the database files.
5. eHealth checks the system on which you are performing the load to make sure that it has sufficient space and that the number of files per tablespace is sufficient for the loaded database.
   - If the system has sufficient space, eHealth loads the saved files into the new database.
   - If a disk does not contain enough space, eHealth displays an error message that identifies the disk, the amount of additional space that is needed, and the files that exist on that disk. If this occurs, add another datafile to the tablespaces on that disk, or move one of the tablespaces to another disk that has more space.

6. Once the load database process finishes, restart the eHealth server.

**Move Distributed eHealth Databases**

You cannot load a database backup that was created on a Distributed eHealth System onto a Distributed eHealth Console (or vice versa). If you have a Distributed eHealth system, you must replicate the object information after you load the database. For more information about this process, see the *Distributed eHealth Administration Guide*.

If you are loading the database into a Distributed eHealth System, see the *Distributed eHealth Administration Guide* for instructions on synchronizing the system after the load finishes.

**Stop the Database**

If you are shutting down the eHealth system, you should first stop the database so that connections can be closed in an orderly way before shutdown. You may also need to stop the database if you change the eHealth system hostname, or when troubleshooting system problems.

The `nhStopDb` command stops the database, provided that other processes are not still connected to it. Before you run this command, you must stop these other processes. You can use the `nhStartDb` command to restart the database manager, as described in the *eHealth Commands and Environment Variables Reference Guide*. The database manager automatically starts when you reboot the workstation.

To stop the database manager, you can use any of the following methods:

- A normal shutdown waits for all users to disconnect, prohibits new users from connecting to the database, closes and dismounts the database, and then shuts down the instance. This action is the default.
- An immediate shutdown backs out any uncommitted user transactions, logs out all users, and then shuts down the database. A recovery is not required upon startup.
- An abort shutdown stops the database just as it is, with operations pending or not; it requires a recovery on startup. You should only use this method for emergencies.
Before shutting down a UNIX workstation, always stop the database server.

**To stop the database manager**

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:
   
   ```
   nhServer stop
   ``
   
   The eHealth server stops.
3. If you are on a UNIX system, log in as root.
4. Enter one of the following commands, where `eHealth` denotes the eHealth home directory and `option` denotes the type of shutdown (normal, immediate, or abort):
   
   ```
   /eHealth/bin/nhStopDb (on UNIX systems)
   nhStopDb option (on Windows systems)
   ```

**Establish Database Security**

To make sure that your eHealth database is secure, follow these guidelines:

- Every time you load a database, change the database passwords for all eHealth admin-level accounts.
- Keep archived copies of your database saves in a secure location. That is, make sure that you save the database in a directory that is owned by a secure user who has read-only permissions. (Any users who have access to the saved database can restore it and view all of the data that it contains.)
- Make sure that the eHealth user does not have database administrator permissions for the Oracle database.
- Change user passwords and manage user permissions by using the `nhManageUsers` command. For more information, see the next section, “Change User Passwords.”
- Change passwords for the following default accounts: sys, system, dbsnmp, and NH_USER. To obtain access to a list of all database users, see page *Obtain a List of All Accounts on page 141*.

**Important!** Change passwords only using eHealth tools. If you change passwords directly through Oracle, it could disable eHealth.

**Change User Passwords**

When the installation program creates the eHealth database, it changes the passwords of the Oracle sys and system accounts to eHealth to maintain system security. You can use the `nhManageUsers` command to change these passwords. If you choose to change these passwords to provide additional security, you must remember the new passwords and supply them when necessary.
You can add new users and set their permissions. The eHealth administrator can add, list, modify, and delete user and system passwords for all users. Other users can edit their own passwords only. When users connect to the database (by running commands to add new users, perform database loads, or destroy the database), eHealth prompts them to supply a password. If a user does not have the appropriate permissions to perform the specified action, eHealth returns an error message and prevents the action.

If the password file is lost or corrupted, contact Technical Support for help generating a new file.

**Obtain a List of All Accounts**

Before you change passwords, obtain a list of all user accounts in your system.

**To obtain a list of all accounts on your system**

1. Log in as the eHealth user.
2. Enter the following at the command prompt:
   
   ```
   nhManageUsers -list
   ```

   A list of all database accounts similar to the following appears:

<table>
<thead>
<tr>
<th>Username</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>nhuser</td>
<td>admin</td>
</tr>
<tr>
<td>sys</td>
<td>admin</td>
</tr>
<tr>
<td>system</td>
<td>admin</td>
</tr>
<tr>
<td>cmi04</td>
<td>readOnly</td>
</tr>
<tr>
<td>nhlistener</td>
<td>readOnly</td>
</tr>
</tbody>
</table>

**Manage User Accounts**

You can use the `nhManageUsers` command to change user passwords and privileges, add new users, and list users and their privileges. The following table provides the syntax you can use with the command.

<table>
<thead>
<tr>
<th>Action</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding users</td>
<td>`nhManageUsers -add -user db_account -priv [admin</td>
</tr>
<tr>
<td>Deleting users</td>
<td><code>nhManageUsers -delete -user db_account</code></td>
</tr>
<tr>
<td>Listing user passwords</td>
<td><code>nhManageUsers -showPass -user db_account</code></td>
</tr>
<tr>
<td>Modifying user passwords</td>
<td><code>nhManageUsers -modPass -user db_account</code></td>
</tr>
<tr>
<td>Listing all users and their privileges</td>
<td><code>nhManageUsers -list</code></td>
</tr>
<tr>
<td>Listing user privileges for a single user</td>
<td><code>nhManageUsers -showPriv -user db_account</code></td>
</tr>
</tbody>
</table>
To change a user password

1. Log in as a user with administrator privileges.
2. Change the password by entering the following:
   
   ```
   nhManageUsers -modPass -user db_account
   ```
3. At the prompts, supply the old password and the new password, and then verify the new password.
4. If you have Report Center installed and plan to change the password for the database user named CRN, complete these steps:
   a. Run `eHealth/crn/bin/crconfig.sh` (UNIX) or `crconfig.bat` (Windows).
   b. Navigate to Data Access, Content Manager, eHealth.
   c. Update the User Password.

Create the Database Password File

EHealth recreates the database password file after you perform a load for standard saves. That is, after a standard database load, it resets the password file to use eHealth as the password for all accounts. For universal saves, however, it resynchronizes the password file so that the original password that was in use on the system remains valid even after you load a database. For example, if you load a database with an eHealth user named bsmith, the password of bsmith after the load is the same as it was before the load.

Change the Model Size of the Database

An incorrectly configured database size can impact the performance of the Oracle database. The size of the database is determined during installation, based on information that you enter for the type and number of elements to poll and the number of tablespaces to use for the database.

Your database grows and allocates disk space at a specific rate, based on the number of statistics elements that you have created for it to manage. If you plan to change your database size significantly (for example, if you had originally created a database to manage 5,000 elements and you are now planning to manage 20,000 elements), you may need to change the model size of the database.
**Before changing the model size of the database**

1. Use the eHealth Sizing Wizard to determine whether you have enough disk space to support the number of elements that you want to monitor.
2. Add datafiles to your tablespaces (if necessary) by using the `nhManageDbSpace` command.

**To change the database model size**

1. Log in to the eHealth system as an administrator.
2. Enter the following command to stop the eHealth server:
   ```
   nhServer stop
   The eHealth server stops.
   ```
3. Close eHealth by selecting Console, Quit in the eHealth console.
4. Enter the following at a command prompt, selecting one of the four size options:
   ```
   nhChangeDbModelSize [-small|-medium|-large|-xlarge]
   ```
   For example, to specify that you want to create a medium-sized database, enter the following:
   ```
   nhChangeDbModelSize -medium
   ```
5. Restart eHealth:
   - On Windows systems, select Start, Programs, eHealth #, eHealth.
   - On UNIX systems, enter eHealth from the `/eHealth/bin` directory.

   The `nhChangeDbModelSize` command does not resize existing tables. This command inserts new tables or new rows into existing tables by conforming to the new model size that you specified. Oracle allocates extents when the previously allocated extents do not have any room remaining. If you change the model size, but the existing extents are not used completely, the size of the database does not change. The command adds a new extent using the new size that you specified only after all blocks in existing extents are full.

**Resize the eHealth Database**

If you delete a large part of a database (either by deleting hundreds of elements or removing Report Center and its time-aligned statistics database), the disk space is not automatically returned as “free space.” You should resize your eHealth database to optimize the database disk space usage and regain any space that is no longer needed by the database files.

To regain the disk space, you can export the current database, destroy and recreate the database, and then load the exported database. This creates a new database that is more space-efficient, and returns any unused disk space as free space for the disks on which the database files reside. The process does result in some downtime for the eHealth system while the database is being destroyed and created, and while the database is being loaded. Try to schedule this task to occur on a weekend or during a period of low activity.
To resize the eHealth database

1. Log in to the eHealth system as the eHealth administrator. If the system is a UNIX system, change to the eHealth home directory and source the nethealthrc file to set the environment variables.

2. Export the current eHealth database by using the following command, where `saveDir` is the directory in which you want to save the exported database.
   This command assumes that you intend to reload the database on the current eHealth system and takes advantage of the `-fast` option to reduce the time needed to export the database.

   ```
   nhSaveDb -ascii -fast -compress -p saveDir
   ```

3. After the export process finishes, destroy the current database by using the following command, where `SID` is the name of the eHealth database (usually `eHealth`). For UNIX eHealth systems, you must log in as the root user to complete this step, as well as the following step.

   ```
   nhDestroyDb -s SID
   ```

4. Create a new database using the `nhCreateDb` command.
   The command launches an interactive script that prompts you for information about the database. If you used a layout configuration file (LCF) to specify the database locations and create a tailored database for your environment, use the command `nhCreateDb -l lcfPathname` where `lcfPathname` is the pathname to the LCF file. For UNIX eHealth systems, you must be the root user to complete this step.

5. Load the exported database using the command `nhLoadDb -p saveDir` where `saveDir` is the location of the exported database specified in Step 2.
   After the load finishes, the eHealth database should consume a smaller amount of disk space, and eHealth should report more free space for the database disk locations and tablespaces.

Modify the Oracle Network Configuration

The eHealth installation program automatically configures the network interface for Oracle. However, you may need to modify the configuration if you make network changes. You can use the `nhConfigDbNet` command to modify the Oracle network interface.

The following table provides the syntax that you can use with the command:

<table>
<thead>
<tr>
<th>Action</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the port number</td>
<td><code>nhConfigDbNet -addListener -port portNumber</code></td>
</tr>
<tr>
<td>Modify the Oracle instance (sid)</td>
<td><code>nhConfigDbNet -addListener -sid oracleSid</code></td>
</tr>
<tr>
<td>Modify the listener (listener.ora file)</td>
<td><code>nhConfigDbNet -addListener -listenername listenername</code></td>
</tr>
<tr>
<td>Update the tnsnames.ora file</td>
<td><code>nhConfigDbNet -addTnsNames</code></td>
</tr>
</tbody>
</table>
For detailed information about the nhConfigDbNet command, see the eHealth Commands and Environment Variables Reference Guide.

**To change the port number and oracle SID**

1. Log in as a user with administrator privileges.
2. Enter the following command:

   nhConfigDbNet -addListener -sid oracleSid -port portNumber

**View the Status of the Database**

eHealth provides summary information about the status of the entire database. If your web user account has the appropriate permissions, you can use OneClick for eHealth to do all of the following:

- Check tablespaces (logical storage units that can contain datafiles within an Oracle database).
- Check associated datafiles (physical structures that store the data in the database).
- Review specific information about statistics and conversations data.
- View the contents of the entire eHealth database and the times at which the statistics rollups occurred.
- Review the size and consumption of each tablespace, and the size and status of the disk partitions and datafiles.
- Review the times at which eHealth rolled up as-pollled, rolled-up, and rolled-up top conversations, and the size of these rollups. (To obtain this information, you must install a Traffic Accountant license on your system.)
- Drill down to the Database Alerts message window to identify when problems occurred.
- Drill down to the Job History window to review when all database-related scheduled jobs were run.

**To view the current status of the database**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information and manage the database.
2. In the left pane, click Tasks and Information, System Information, and then double-click Database Status. The Database Status window appears.

**Troubleshoot Database Connection Problems**

If you cannot connect to the eHealth database, perform the following procedure to troubleshoot the problem.
**To connect to the eHealth database**

1. Enter the following command at the command prompt:

   ```
   sqlplus
   ```

2. Enter your database user name and password.

3. If you cannot log in, you do not have access to the database. Verify your user name, password, and permissions. If you do have access to the database, determine whether Oracle is running.

4. If you logged in successfully but cannot connect to the database, check to see if Oracle is running.

5. Enter the following at a command prompt:

   ```
   ps -ef | grep $ORACLE_SID
   ```

6. Check the output of this command for the following processes:

   - pmon
   - smon
   - dbw
   - arc
   -ckpt
   - rec

7. Do one of the following:

   - If these processes are not running, go to Step 8 to start the database.
   - If the processes are running (UNIX only), do the following:
     a. Enter the following command and check for a list of Oracle shared memory segments:

        ```
        ipcs -a
        ```

        If the shared memory segments are not present, the database instance is either not started or is in an inconsistent state.
     b. If Oracle is running and you still cannot connect to the database, start the database.
     c. Enter the following at the command prompt:

        ```
        nhStartDb
        ```

        d. Verify that the database has started.
        e. Try to connect to the database.

8. If you cannot start the database and its processes are not running, verify that it exists.
9. Verify that the parameter initialization file exists:
   - On UNIX systems, look for the following file:
     
     `$ORACLE_HOME/dbs/initORACLE_SID.ora`
   - On Windows systems, look for the following file:
     
     `%ORACLE_HOME%\database\initORACLE_SID.ora`

10. Change directory to the location in which you installed the database tablespace. For example, if you installed the tablespace in `D:\database`, enter the following:

    `cd D:\database`

11. Verify that the following files exist in the same directory:

    `databaseDir\ctl\control.ctl.ora`
    `databaseDir\oradata\system*.dbf`
    `databaseDir\oradata\index*.dbf`
    `databaseDir\oradata\rds*.dbf`

12. If these files do not exist, you must install the database. For instructions, see the *eHealth Installation Guide*.

13. If these files exist, your database is installed. If you still cannot connect to the database, force it to restart by doing the following:
   a. Enter the following at a command prompt:
      
      `sqlplus "/ as sysdba"
      `shutdown immediate`
   b. Wait 30 seconds for the database to shut down; then enter the following commands:
      
      `startup`
      `exit`
   c. Restart the Oracle database service by entering `nhStartDb` from the `/eHealth/bin` directory.
   d. Restart your system.

14. If the database still does not start, force it to start by doing the following:
   a. Stop the Oracle database service by selecting Start, Control Panel, Services, selecting OracleServiceORACLE_SID, and clicking Stop.
   b. Recreate the service by entering the following commands:
      
      `oradim -delete -sid ORACLE_SID`
      `oradim -new -sid ORACLE_SID -startmode auto -pfile ORACLE_HOME\database\initORACLE_SID.ora`
   c. Enter the following at a command prompt:
      
      `sqlplus "/ as sysdba"
      `shutdown immediate`
   d. Wait 30 seconds for the database to shut down, then enter the following commands:
      
      `startup`
      `exit`
e. Restart the Oracle database service by selecting Start, Control Panel, Services, and then select OracleServiceORACLE_SID and click Start.

f. Restart your system.

If you still cannot connect to the database after performing these procedures, contact Technical Support.

Troubleshoot Database Disk Space Problems

If the disks containing the eHealth database run low on space, the following problems can occur:

- At-a-Glance reports for the eHealth system can show disk space problems.
- The eHealth console can indicate report failures.
- Traps from SystemEDGE and the Oracle AIM can reveal Oracle space problems.
- The database manager or eHealth can fail to start.

Disk space problems can be caused by a fragmented database, unnecessary files that consume large amounts of space, or a disk that is unable to accommodate the volume of eHealth activity.

These symptoms may also indicate that you need to add a datafile to a tablespace, move a datafile from one tablespace to another, or change a setting in the initialization parameter file. This file is located in the database (Windows) or dbs (UNIX) subdirectory of $ORACLE_HOME and is named initORACLE_SID.ora.

Examine the Disks

To determine whether a disk is large enough for the volume of eHealth activity that you are experiencing, use OneClick for eHealth to examine the amount of available space on the disk.

**To determine available disk space on the disk**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information and manage the database.

2. In the left pane, click Tasks and Information, System Information, and then double-click Database Status.

   The Database Status window appears.

3. Examine the amount of free space on the disk. If the disk has less than 1 MB free, the disk is full.
4. Compare the amount of space used by the database to the available disk space to determine what is consuming disk space:
   - If the two values are very close, the database is using most of the space. Allow the database manager to reclaim some of its space.
   - If the database is not using most of the space, clean up the disk.
   - If the command indicates that the disk is not full, you may have a full tablespace.

How to Reclaim Disk Space

Before you increase the size of your physical disks, make sure that your current disk space is being used efficiently. If the database is growing significantly, taking the following actions to reclaim disk space will not alleviate the need for more disk space, but they will maximize existing disk space.

To reclaim disk space, follow these steps:
1. If the database is consuming most of the disk space, do the following:
   - Make sure that the data rollup jobs and other scheduled jobs are running regularly.
   - Shut down and restart the database to allow the database manager to reclaim some of its space.
   - Move datafiles to other disks.
2. If other (non-database) files are consuming a large amount of disk space, free space by doing the following:
   - Delete core files (UNIX systems only).
   - Delete temporary files.
   - Delete old report files.
   - Use the nhExpire command or the Scheduled Jobs window in the OneClick for eHealth console to eliminate old jobs.
   - Make sure that your disks contain only files that belong to eHealth and Oracle. Delete any other applications and related files. Your eHealth system should be dedicated to eHealth.

   **Important!** If you delete files that you do not recognize, you may damage the eHealth system.

Delete Core Files

Core files are generally large. To save disk space, you should delete them on a regular basis unless you are using them to troubleshoot application problems.

To identify core files, enter the following command, where `/disk` is the pathname for the database disk:

```
find /disk -name core -print
```
Delete Temporary Files and Old Report Files

When you generate eHealth reports using the console or the eHealth Web user interface but do not save them, eHealth saves the files in the `/eHealth/tmp` and `/eHealth/web/tmp` directories, respectively. When you save reports as ASCII, PostScript, or portable document format (PDF), eHealth saves the files in the `/eHealth/output` directory by default. When you output eHealth reports to the eHealth Web user interface, the system saves them in the `/eHealth/web/output` directory.

To free disk space, you can use the following two methods:

- Run the nhExpire command to delete old report files and temporary files from the output, web, and tmp directories. For more information on this command, refer to the `eHealth Commands and Environment Variables Reference Guide`.

- Clean up these directories on a regular basis by modifying the Delete Old Reports job to change the number of days that eHealth retains the reports and temporary files, as well as when the job runs. To maintain disk space and clean up old files, eHealth automatically runs this job at 6:00 A.M. daily to delete the following files:
  - ASCII, PDF, or Postscript report files in the output directory that are older than 31 days
  - Temporary files in the `/eHealth/tmp` and `/eHealth/web/tmp` directories (including PDF files) that are older than four days
  - Web-based reports in the directories listed in the following table that are older than 31 days

<table>
<thead>
<tr>
<th>Report</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health, Service Level, and Top N</td>
<td><code>/eHealth/web/output/groups</code></td>
</tr>
<tr>
<td>Service Level</td>
<td><code>/eHealth/web/output/groupLists</code></td>
</tr>
<tr>
<td>Trend and At-a-Glance</td>
<td><code>/eHealth/web/output/users</code></td>
</tr>
<tr>
<td>Traffic Accountant</td>
<td><code>/eHealth/web/output/views</code></td>
</tr>
</tbody>
</table>

Reduce Demands on Disk Space

If you are unable to free significant space on your disk by reclaiming disk space, the size of your disk might be inadequate for the volume of eHealth activity.

To reduce the demands of eHealth on disk space, you could do one of the following:

- Set a longer polling interval.
- Move the database to a new disk.
- Move datafiles to tablespaces that are located on other disks.
Add a Datafile

When a tablespace is full, you can add another datafile as long as the amount of disk space that you specify for the datafile size is available.

If you encounter any of the following problems, a full tablespace might be the root cause:

- Messages in the $ORACLE_HOME/admin/bdump/$ORACLE_SID/alert_$ORACLE_SID.log file stating that you are out of disk space
- Oracle error message: ORA-1652: unable to extend temp segment error
- Oracle warning messages that you are out of disk space or have exceeded the maximum number of blocks
- A data analysis failure with an Oracle out of disk space error

To troubleshoot these errors, check disk space. After checking disk space, you may be able to resolve the errors by adding a datafile to extend the tablespace or moving a datafile to a device with more free disk space. However, if you are experiencing errors and a tablespace has more than one datafile and at least one datafile is not approaching the 32 GB limit, contact Technical Support.

The following procedure explains how to use the nhManageDbSpace command to add a datafile to a tablespace. For complete instructions on using this command, see the eHealth Commands and Environment Variables Reference Guide.

To add a datafile of 100 MB to the NH_DATA01 tablespace

1. Enter the following command, where /export/blue11/oradata/eHealth is the path to the new datafile and eHealth is the name (session ID) of the eHealth database:

   \`nhManageDbSpace -add -newPath /export/blue11/oradata/eHealth -tablespace NH_DATA01 -size 100\`

2. Confirm the location of the new datafile by reviewing the LCF:

   \`more /opt/eHealth/oracle/database/blue_eHealth.lcf\`

   where blue is the name of the system and eHealth is the name of the database.

3. If you destroy and recreate the database at a later time, provide the LCF as input to the nhCreateDb command. This enables the command to create a database with the correct number of datafiles.

Move a Datafile

If the NH_INDEX, NH_USERS, NH_DATA01, or NH_DATA02 tablespace is running out of disk space, you can use the nhManageDbSpace command to move the datafile or datafiles to a tablespace on a larger disk on the eHealth system. If possible, you should try to keep the largest tablespaces (NH_INDEX, NH_DATA01, and NH_DATA02) on separate disks or partitions. NH_INDEX
should reside on the largest disk with the highest input/output performance. NH_DATA01 should reside on the next largest disk with the next highest input/output rate. Apply these guidelines for NH_DATA02.

**Important!** Moving a datafile requires stopping the eHealth server. Only perform this procedure when users do not need to access eHealth reports, the eHealth Web console, and Live Health.

**To move a datafile for the NH_INDEX01 tablespace**

1. View the status of the database in the OneClick for eHealth Console to confirm the path to the datafile that you want to move.
2. Log in to the eHealth system as an administrator.
3. Enter the following command to stop the eHealth server:
   
   ```
   nhServer stop
   ```

4. Test the command syntax and confirm that adequate space exists by entering the following command:

   ```
   nhManageDbSpace -evaluate -move -datafile /export/myHost/oradata/eHealth/NH_INDEX01.dbf -newPath /export/myHost1
   ```

5. If the output does not include any errors, move the datafile by entering the following:

   ```
   nhManageDbSpace -move -datafile /export/myHost/oradata/eHealth/NH_INDEX01.dbf -newPath /export/myHost1
   ```

6. Review the output to make sure that the command has moved the datafile:

   ```
   Moving file ...
   Created: /export/myHost/eh570/oracle/database/myHost_eHealth.lcf.2004-08-11-0842
   Updated: /export/myHost/eh570/oracle/database/myHost_eHealth.lcf
   ```

7. After moving the datafile, the nhManageDbSpace command renames the existing layout configuration file and generates a new one. **myHost_SID.lcf** is always the name of the latest LCF where **myHost** represents the system name and **SID** represents the database name.

8. Confirm the new location of the NH_INDEX01.dbf datafile by entering the following:

   ```
   grep NH_INDEX $NH_HOME/oracle/database/myHost_eHealth.lcf
   ```

9. Start the eHealth server by entering the following:

   ```
   nhServer start
   ```

   If you destroy and recreate the database at a later time, make sure that you provide the LCF as input to the nhCreateDb command. This enables the command to create a database with the correct number of datafiles.
This chapter contains the following sections:

- eHealth’s Self-Monitoring Capabilities
- Track OneClickEH Administration Changes
- Track Element Changes in the Database
- Monitor Scheduled Job History
- Monitor Web Activity
- Monitor Database Alerts
- Manage eHealth System Files
- Monitor eHealth System Processes

**eHealth’s Self-Monitoring Capabilities**

To enable eHealth to collect data on your resources, it is important to monitor the system logs and processes on a regular basis. eHealth provides tools that you can use to determine if processes are operating as expected and to identify problems so that you can take corrective action. This chapter provides an overview of these monitoring tools. The OneClick for eHealth (OneClickEH) administrative console provides useful monitoring capabilities that you can use to manage eHealth processes:

- **The eHealth History** feature allows you to quickly view all historical activity that has occurred within a specified time frame. It provides you with immediate access to system, web server, and OneClickEH activity logs; scheduled job history; and database alerts. With this information, you can easily identify current or potential problems that are developing with processes and address issues before they prevent eHealth from monitoring your resources.

- **The Setup feature** allows you to control the eHealth server and the poller, and provides you with an advanced logging capability for troubleshooting configuration problems.

- **The System Information feature** provides you with immediate access to the entire eHealth file structure for your primary system directories. You can display the contents of each system directory and determine when the files were last changed. You can also view the status of your eHealth database, monitor server processes, and review environment variable settings and license keys.
Track OneClickEH Administration Changes

It is important to monitor system logs and processes on a regular basis to enable eHealth to collect data on your resources without interruption. eHealth provides tools that you can use to monitor processes and identify problems so that you can take corrective action. You can identify the administrators who recently made changes to the database using OneClickEH, the tasks that they performed, when the activity took place, and the IP addresses of the clients on which the tasks were performed. In the OneClickEH Activity window, informational messages appear in white, warnings appear in orange, and errors appear in red.

To monitor administration changes that have occurred

1. **Access the OneClickEH Console** and log in to the eHealth system as a web user who has permission to view eHealth logs and history.
   
   The eHealth Status Summary window appears.

2. In the left pane, select Tasks and Information, eHealth History, and then click OneClickEH Activity.
   
   OneClickEH displays a full log of activity that has occurred within the last hour.

3. Scan the list of messages and review warnings (in orange), errors (in red), and informational messages (white). Do any of the following:
   
   a. Click a tab at the top of the table.
      The screen refreshes to show activity for the selected time period.

   b. Confirm that processes are running as expected, and pinpoint when problems occurred.

   c. If necessary, reorder or resize the columns, and click a column to sort the data.
      The data reorders based on timestamp, type, or content.

   d. Right-click to copy and paste specific entries, export the data to a file, or print the data.

   e. Click the Log Administration tab.
      The OneClickEH Activity Log Administration window appears.

   f. Review the amount of disk space that the OneClickEH activity log is consuming.

   g. If the log file is becoming too large and you do not need to retain the data, click Clear or reset the default.
      The screen refreshes to show an increase in the amount of available disk space.
Track Element Changes in the Database

To make that eHealth can successfully collect data on your resources, as a best practice, monitor the element changes that administrators have made to the database through OneClickEH and the eHealth console. The pollerAudit.date.time.log file identifies the users who performed the actions and the changes that they made, which allows you to pinpoint when problems occurred.

To track element changes that have occurred

1. **Access the OneClickEH Console** and log in to the eHealth system as a web user who has permission to view to view eHealth logs and history.
   
   The eHealth Status Summary window appears.

2. In the left pane, select Tasks and Information, eHealth History, System Information.

3. Search through the Server Files folder for the Log subfolder, and open the pollerAudit.date.time.log file.

   OneClickEH displays the contents of the log file.

   - Date and time of the change, and the time zone in which it was made.
   - Name of the eHealth user who made the change.
   - Source of the change (e indicates element configuration, i indicates interactive discover, a indicates scheduled discover, and u indicates an unspecified process).
   - Unique numerical identifier that eHealth assigns to the element.
   - The action that was taken (that is, element was added, deleted, modified, or disabled).
   - Name of the element.
   - Changes that were made.

4. Review each change.

Track System Events

Immediately after you log in to the OneClick for eHealth console, the Status Summary window lists the total number of system events, warnings, errors, and informational messages that have been generated by the eHealth system over the past 24 hours. System messages can describe routine activity and indicate when system events occur such as the console initialization. They also identify operational errors relating to groups, the database, or user management. You can use this information to confirm that processes are running as expected, and pinpoint when problems occur. In the OneClickEH System Messages window, informational messages appear in white, system events appear in blue, and errors appear in red.
To track system events that have occurred

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, System Messages.
   OneClickEH displays a full log of activity that has occurred within the last hour.
3. Scan the list of messages to identify events (in blue) and errors (in red). Do any of the following:
   a. Click a tab at the top of the table to view activity for a particular time period.
   b. Confirm that processes are running as expected, and pinpoint when problems occurred.
   c. If necessary, reorder or resize the columns, and sort the data based on timestamp, type, or content.
   d. Right-click to copy and paste specific entries, export the data to a file, or print the data.

Monitor Scheduled Job History

Using the OneClick for eHealth console, you can manage your scheduled jobs by identifying jobs that have failed, those that have been failing repeatedly over time, or those that are taking much longer than usual to run. The Job History log shows the status of all scheduled system jobs that eHealth has run recently or during a specified time period and identifies their status.

Important! OneClickEH represents scheduled job times in the time zone of the client system. If the server and client are in different time zones, this may be confusing.

To monitor scheduled job history

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information and manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job History.
   OneClickEH displays a full log of activity that has occurred within the last hour.
3. (Optional) Do any of the following:
   a. Click a tab at the top of the table to view job activity for a particular time period.
   b. Scan the list of jobs to identify those that have finished (in white), those that have been killed (in orange), and those that have failed (in red).
c. If necessary, reorder or resize the columns, and sort the jobs based on status or duration.

d. Right-click to copy and paste specific job data, export the data to a file, or print the data.

e. Run a specific job on demand by copying its command from the Command column into a Command Prompt window.

f. Display a summary of the information pertaining to a particular job by double-clicking it.

Monitor Web Activity

Using the OneClickEH Web Activity log, you can quickly identify the administrators who recently performed tasks, the types of tasks that they performed, when the activity took place, and the client system on which the activity occurred. By correlating errors with the activity, you can use this information to quickly identify when and how problems occurred with the eHealth Web server and take action to rectify the situation. Messages can convey general information about activity, identify errors, or warn of potential problems.

To track web server activity

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.

   The eHealth Status Summary window appears.

2. In the left pane, select Tasks and Information, eHealth History, Web Activity.

   OneClickEH displays a full log of activity that has occurred within the last hour.

3. Scan the list of messages to identify events (in blue) and errors (in red). Do any of the following:
   
a. Click a tab at the top of the table to view activity for a particular time period.

   b. Identify the administrators who recently performed tasks, the types of tasks that they performed, when the activity took place, and the client system on which the activity occurred.

   c. Correlate the errors with the activity to quickly identify when and how problems occurred with the eHealth web server, and then take action to rectify the situation.

   d. If necessary, reorder or resize the columns, and sort the data based on timestamp, type, or content.

   e. Right-click to copy and paste specific entries, export the data to a file, or print the data

   f. (Optional) Select the eHealth Web UI link in the left pane, log in to the eHealth Web user interface as an administrator, and click Access Logs under eHealth Management on the Administration page.

   The Access Logs page appears.
4. Do the following:
   a. Generate a detailed list of all connections that all or specific users have made to the web server, all or specific web pages that users have accessed, and a specific time and date range during which the access occurred.
   b. Display summary statistics of individual connections to the web server (that is, for each report page).

Monitor Database Alerts

The Database Alerts log displays all messages generated by the eHealth database over a specified period of time. Messages are sent to the operator console during daily database operations such as shutdown, startup, and archiving, and when errors are generated that cause trace files.

To monitor database activity

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History folder, System Messages, Database Alerts.
   OneClickEH displays all messages generated by the eHealth database over the last hour.
3. Do the following:
   a. Review the messages that were generated as a result of database operations.
   b. Identify when errors occurred.
   c. (Optional) Right-click to copy and paste specific data, export the data to a file, or print the data.

Manage eHealth System Files

By navigating through the OneClickEH Server Files folder, you can access the entire eHealth file structure for your primary system directories (eHealth, Database, and Web Content). By reviewing the file properties, you can identify files that are consuming a significant amount of disk space and determine which files were changed at the time that a problem occurred.

To manage eHealth system files

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, System Information, Server Files.
   The window refreshes and then displays the eHealth system file folders.
3. Right-click the file name and select View File, or double-click the file name in the window.
   OneClickEH displays a spreadsheet of all eHealth processes.

4. Do the following:
   a. Review the size, read/write access settings, last modified date, and owner of each file contained in the three primary system directories.
   b. Identify files that are consuming a significant amount of disk space and determine which files were changed at the time that a problem occurred.
   c. (Optional) Right-click to copy and paste specific data, export the data to a file, or print the data.
   d. Take corrective action to resolve the problems, as necessary.

**Monitor eHealth System Processes**

To make sure that eHealth is able to collect data on your resources, it is important to monitor the system processes on a regular basis and identify problems so that you can take corrective action.

**To monitor eHealth system processes**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view system information.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, System Information, Server Processes.
   OneClickEH displays a spreadsheet of all eHealth processes.
3. Find a specific process by entering text in the Filter table by field at the top of the OneClickEH console screen, and then do the following:
   a. Review the amount of physical memory used by each process, the CPU, and the state of the process.
   b. Click the State column to quickly identify processes that have stopped unexpectedly.
   c. (Optional) Right-click to copy and paste specific data, export the data to a file, or print the data.
   d. Take corrective action to resolve problems, as necessary.
Chapter 9: Managing Scheduled Jobs

This chapter contains the following sections:

- **eHealth Scheduled Job**
- **The eHealth Job Scheduler**

**eHealth Scheduled Job**

An eHealth scheduled job is a process that the eHealth job scheduler runs on a regular basis to facilitate the administration of your eHealth system. eHealth provides multiple default scheduled jobs to help you administer your eHealth system. Some are specific to Traffic Accountant systems, Distributed eHealth Systems, and the Live Exceptions application, while others maintain the health of your database and automate the data analysis process on which eHealth reports are based. Most scheduled jobs have a command line interface (CLI) counterpart, while some are internal processes that you cannot run manually through the CLI. Almost all jobs are enabled by default upon installing eHealth, but most are modifiable through the scheduler.

**The eHealth Job Scheduler**

The **eHealth job scheduler** is an eHealth feature that automates several maintenance tasks that eHealth administrators need to run on a regular basis to keep the eHealth system running effectively. The job scheduler runs these tasks automatically as scheduled “jobs” so that you do not have to repeatedly perform them manually. For those jobs that run only once daily, the scheduler runs them outside of the normal business day (late in the evening, in the middle of the night, or very early in the morning) so that the processes do not interfere with the daily collection and processing of data.

- Through the OneClickEH user interface, you can manage default system jobs, report jobs, and discover jobs in the following ways: modify the job schedule to suit the particular needs of your eHealth site, enable or disable the jobs, and delete the jobs when you no longer need them. From the OneClickEH scheduler, you can also create new discover jobs.
The eHealth Job Scheduler

- Through the eHealth console, you can create Database Save scheduled jobs and report scheduled jobs for any report type. You can also modify certain parameters of scheduled report jobs.
- Through the CLI, you can add new jobs and create customized jobs to run frequently-used scripts on a regular basis.

View Scheduled Jobs

Through the OneClick EH interface, you can view a list of all scheduled jobs that are run for your eHealth system.

To view scheduled jobs

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
   OneClickEH displays a list of all system jobs that are scheduled to run automatically, along with the time, status (enabled or disabled), time zone (if applicable), and associated command. Any jobs that are currently disabled are grayed-out in the table.
3. Click a column header to sort the jobs in the list, or select a tab to display a particular type of job.
   OneClickEH reorders or filters the list.

How to Monitor Scheduled Jobs and Identify Problems

Because some scheduled system jobs help you manage database growth and changes and keep your eHealth system up-to-date, it is important to track any unusual time lags or unexplained failures and investigate the problems as soon as possible. As a best practice, you should monitor your scheduled jobs to identify problems.

1. Use the OneClick for eHealth console to log in to your eHealth system as an administrator who has permission to manage scheduled jobs.
2. From the eHealth Status Summary page for your eHealth system, drill down to the Job History page.
3. Sort the information in the table to identify jobs that have failed (red), those that stopped before finishing (orange), those that have been failing repeatedly over time, or those that are taking much longer than usual to run.
   Important! Jobs show a status of Killed if you stop the process manually or eHealth queues the job but does not run it before the DB Maintenance job runs. When the DB Maintenance job runs, it kills any jobs in the queue.
4. Identify any unusual time lags or unexplained failures.
5. Investigate the problems as soon as possible by reviewing the log files in the log directory of your eHealth installation.
6. Troubleshoot the problems by disabling the jobs temporarily or changing the default schedule (time, day, and frequency).

7. (Optional) Copy the text in the Command column and paste it into a command prompt window, and then press Enter.

Run a Scheduled Job on Demand

Through the OneClickEH console, you can run a scheduled system, report, or discover job on demand without having to use the CLI.

To run a scheduled job on demand

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
   OneClickEH displays a list of all system jobs that are scheduled to run automatically.
3. Sort through the list to find the job that you need to run.
4. Copy the text in the Command column, paste it into a command prompt window, and then press Enter.
   eHealth runs the scheduled job on demand.

Review Scheduled Job Log File

Through the OneClickEH console, you can investigate problems that have occurred with scheduled jobs by reviewing the log files.

To access a scheduled job log file

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
   OneClickEH displays a list of all system jobs that are scheduled to run automatically.
3. Right-click the job for which you want to review the log file, and select Find Log File.
   The window refreshes and opens the designated log file.
Enable and Disable Scheduled Jobs

When you need to troubleshoot problems with your eHealth system or perform an upgrade, you can use OneClickEH to temporarily disable system jobs, report jobs, or discover jobs that are scheduled to run during that time. When you disable a job, it remains on the list of scheduled jobs, but it no longer runs.

**Important!** You should not disable the Statistics and Conversations Rollup jobs or the Delete Temporary Tables job unless directed to do so by Technical Support. If you disable these jobs, your database could quickly consume available disk space. As a best practice, do not disable the Live Exceptions Baseline job; it immediately affects alarms processing, which can result in skewed data.

**To enable or disable a scheduled job**

1. Use the OneClick for eHealth console to log in to your eHealth server as an administrator who has permission to manage scheduled jobs.
2. Double-click the Job Scheduler folder in the tree, and then click Scheduled Jobs.
   
   The Scheduled Jobs window appears with all jobs listed in the order in which they are scheduled to run.
3. Do one of the following:
   - Select the jobs, right-click, and select Disable, and then click OK.
   - Select the jobs, right-click, and select Enable, and then click OK.
   
   eHealth disables or enables the selected jobs.

Modify a Scheduled Job Using OneClickEH

You can use the OneClickEH job scheduler to change default scheduled system jobs, discover jobs, and report jobs to run on other days or at other times, and change other job parameters.

**Important!** To modify some parameters of report scheduled jobs, you must use the eHealth console.

**To modify a scheduled job using OneClickEH**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
3. Select a tab.
   
   The selected Scheduled Job window for that job type appears.
4. Select the job that you want to modify, right-click, and select Edit Job. The Job Properties window appears.
5. Modify the parameters of the job and the schedule, and then click OK. eHealth saves the changes and runs the job with the specified parameters.

Modify a Scheduled Job Using the CLI

To modify some default scheduled jobs, you need to use the nhSchedule command. You can change a job to run on a certain day of the week or month, or at a particular frequency. However, you cannot specify all of these attributes at the same time. For example, by default, the Element Configuration Backup job runs every four hours, but you can change it.

To use the CLI to modify a scheduled job

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
3. Note the job ID, and then select Start, Run.
   The Run dialog appears.
4. Specify cmd and click OK.
   A command prompt window opens.
5. At the command line, specify the nhSchedule command, along with the Job ID, the schedule for the job, and, optionally, any arguments associated with the command. For example, to schedule the job to run every 12 hours, beginning at 5.30 p.m., enter the following:

   \[\text{nhSchedule -modify 100019 -time "5:30 PM" -period 12}\]

   \textbf{Note:} For detailed instructions on using nhSchedule and the complete syntax of the command, see the \textit{eHealth Commands and Environment Variables Reference Guide}.

Add a Scheduled Report Job

As an eHealth administrator, you can use the eHealth console’s job scheduler to create scheduled report jobs for every standard type of report. Because Health and Service Level reports can take a long time to run, you might want to schedule them to run during off-peak hours. With the exception of the additional Schedule options, the Add Scheduled Report dialog for a report type is exactly the same as its Run Report dialog counterpart. Regardless of the report type that you choose, the basic procedure for adding a scheduled report job is the same across all types.
To schedule a Health report job

1. Log in to the eHealth console as an administrator.
   
   **Note:** If you log in to eHealth remotely and your eHealth system is configured to run in a High Availability environment, specify the shared hostname or shared IP address for your system rather than the specific eHealth system name.

   The eHealth console appears.

2. Select Setup, Scheduled Jobs.
   
   The Scheduled Jobs dialog appears.

3. Select Add Health from the list.
   
   The Add Scheduled Health Report dialog appears.

4. In the Add Scheduled Report dialog, do the following:
   a. Select the subject of the report.
   b. Specify a time range for the report.
   c. (Optional) Specify a time zone.
   d. Select the format in which you would like to output the report.
   e. Set the schedule for the job.
      
      If you specify 31 in the Day of the Month field, the reports will only run on months that have 31 days. To schedule a report for the end of the month, specify the first day of the month.
   f. Click OK.

   eHealth adds the report job to its scheduled job list and runs the job at the scheduled time.

   **Note:** You can use OneClickEH to monitor status of the report job and modify the schedule, but you must use the eHealth console to modify all other parameters of the report job.

Modify a Report Scheduled Job Using the eHealth Console

You can use the OneClickEH job scheduler to change the schedule properties of report scheduled jobs; however, you must use the eHealth console to change all other parameters.

To modify a scheduled report job using the eHealth console

1. Log in to the eHealth console as an administrator.

   **Note:** If you log in to eHealth remotely and your eHealth system is configured to run in a High Availability environment, specify the shared hostname or shared IP address for your system rather than the specific eHealth system name.

   The eHealth console appears.
2. Select Setup, Scheduled Jobs.
   The Scheduled Jobs dialog appears.

3. Select the scheduled report job that you want to modify, and then click Modify.
   The Modify Scheduled Report Job dialog appears.

4. Do the following:
   a. Change the subject of the report.
   b. Modify the time range for the report.
   c. (Optional) Specify the time zone.
   d. Change the format in which you would like to output the report.
   e. Change the schedule for the job.
      If you specify 31 in the Day of the Month field, the reports will only run on months that have 31 days. To schedule a report for the end of the month, specify the first day of the month.
   f. Click OK.

Remove a Scheduled Job on a Standalone eHealth System

You can delete a default scheduled job provided by eHealth by running the nhSchedule command.

**Important!** Use caution in deleting any scheduled jobs that help you manage the growth of your eHealth database. Your database can grow significantly in a short period of time.

To remove a scheduled job on a standalone eHealth system:

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, eHealth History, Job Scheduler; then double-click Scheduled Jobs.
3. Note the job ID.
4. Select Start, Run.
   The Run dialog appears.
5. Specify cmd and click OK.
   A command prompt window appears.
6. At the command line, enter the following:

   ```
nhSchedule -delete 100019
   ```

   eHealth removes the scheduled job.
Remove a Scheduled Job on a Distributed eHealth System

When managing scheduled jobs on Distributed eHealth systems, you can use additional arguments to indicate the specific cluster systems that have the jobs you want to remove.

To remove a scheduled job on a specific eHealth system in a cluster:

1. Select Start, Run.
   The Run dialog appears.
2. Specify cmd and click OK.
   A command prompt window appears.
3. At the command line, enter the following, where *systemName* is the name of the eHealth system:

   \[
   \text{nhSchedule} \; \text{-host} \; \text{systemName} \; \text{-delete} \; 100019
   \]

   eHealth removes the job from the specified eHealth system in the cluster.

Remove a Scheduled Job on a Distributed eHealth System

When managing scheduled jobs on Distributed eHealth systems, you can use additional arguments to indicate the specific cluster systems that have the jobs that you want to remove.

To remove a scheduled job on a specific eHealth system in a cluster

1. Select Start, Run.
   The Run dialog appears.
2. Specify cmd and click OK.
   A command prompt window appears.
3. At the command line, enter the following:

   \[
   \text{nhSchedule} \; \text{-host} \; \text{systemName} \; \text{-delete} \; 100019
   \]

   eHealth removes the job so that it no longer runs.

To remove a scheduled job on all eHealth systems in a cluster except the local system

1. Select Start, Run.
   The Run dialog appears.
2. Specify cmd and click OK.
   A command prompt window appears.
3. At the command line, enter the following:

   \[
   \text{nhSchedule} \; \text{-cluster} \; \text{-delete} \; 100019
   \]

   eHealth removes the job on all eHealth systems in the cluster except the local system.
To remove a scheduled job on all eHealth systems in a cluster

1. Select Start, Run.
   The Run dialog appears.
2. Specify cmd and click OK.
   A command prompt window appears.
3. At the command line, enter the following:

   ```
   nhSchedule -all -delete 100019
   eHealth removes the job on all systems in the cluster.
   ```

Create a Customized Scheduled Job to Automate a Script

To expedite the administration of your eHealth system, you can customize a scheduled job to automatically run any eHealth command that you can run at the command line. If you already run a command regularly with specific arguments, you can use that predefined script to create a customized scheduled job that will generate the script on a regular basis.

To prevent jobs with high resource needs from running simultaneously, you need to define a load value for each job so that intrusive or critical jobs are able to run with more resources and finish quickly and successfully. As with other jobs, you can schedule the job to run on a certain day of the week or month, or at a particular frequency, but you cannot specify all of these attributes at the same time.

To customize a scheduled job to automate a script

1. Define the job type at the command line by using the following syntax:

   ```
   nhSchedule -defineType "type" -load loadValue -cmd commandSyntax
   ```

   where `type` is the name of the script that you want to schedule, `loadValue` is the percentage of system resources that you expect it to use while running, and `commandSyntax` is the actual syntax of the command that you want to automate (for example, `-cmd 'c:\home\bin\chkDskSpc'`).

2. Schedule the job at the command line by using the following syntax:

   ```
   nhSchedule -schedule "JobType" -time "x:xx AM" -daily nnnnnnnn
   ```

3. (Optional) Modify one or more attributes of the job type by specifying the `-modifyType` argument along with the same syntax that you used to specify the job type. For example, enter the following to increase the percentage of system resources:

   ```
   nhSchedule -modifyType "Check Disk Space" -load 30 -cmd 'c:\home\bin\chkDskSpc'.
   ```

**Important!** To remove the customized job, run the `nhSchedule` command with the `-deleteType` argument. You can delete only job types that you have created.
Example

For example, if you have a script that examines the amount of free space in the partition in which eHealth is installed, you can define a job type for that script, and then schedule the job to run at 2:30 a.m. every Monday:

```
nhSchedule -defineType "Check Disk Space" -load 10 -cmd 'c:\home\bin\chkDskSpc'
nhSchedule -schedule "Check Disk Space" -time "2:30 AM" -daily nynnnnn
```
Chapter 10: Managing and Monitoring Systems

This chapter contains the following sections:

- System Data Collection
- SystemEDGE Self-Monitoring Features
- Discover System Elements
- System Process Set Configuration
- Process Set Usage
- eHealth Reports for Systems
- Using Live Health with the SystemEDGE Agent

System Data Collection

To manage and monitor systems in your infrastructure, you can configure eHealth to collect data from Unicenter NSM system agents, and run eHealth reports to monitor your systems. As an alternative, you can also configure eHealth to collect data from SystemEDGE agents and use AdvantEDGE View and eHealth to automate systems-management tasks and inventory tracking.

How to Configure eHealth to Collect Data from Unicenter NSM System Agents

You can configure eHealth to collect data from Unicenter NSM system agents, and run eHealth reports to monitor your systems.

To use Unicenter NSM agents to monitor the performance of systems in your infrastructure, follow these steps:

1. Meet the following system requirements:
   - Install eHealth Release 6.1 on any eHealth supported platform and obtain an eHealth System license. This license enables you to discover the agents, run system reports, and apply Live Exceptions profiles to groups of system elements.
Install the eHealth extension software on each Unicenter NSM system agent from which eHealth collects data. This software enables the collection of additional performance data. To verify that you have the latest version, refer to the Certified Devices page (http://support.concord.com/devices/).

2. Obtain a list of the IP addresses of the systems on which the Unicenter NSM system agents are installed.

3. Organize your system elements by creating groups and group lists of related resources. For instructions, see Chapter 5: Organizing Your Element Configuration by Grouping.

4. Run the eHealth discover process by specifying the IP addresses and community strings for the systems on which the agents reside, and select the System technology. For instructions, see Chapter 3: Discovering Resources.

   eHealth searches the specified IP addresses for systems, and when eHealth detects one, it creates a system element. eHealth continuously polls the agents, and when it detects changes, it automatically updates the element information in the eHealth database. If you want to track the impact of individual processes in the system, you can specify the Find Processes option. By default, this option is selected when you select System technology.

5. Run reports on your systems.

   Important! For information on eHealth reporting, see the eHealth Reports User and Administration Guide.

How the SystemEDGE Agent Collects Data

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

You must install the SystemEDGE agent on every workstation or server that you want to monitor. You can then configure SystemEDGE to monitor those systems for variables that you specify. SystemEDGE supports monitoring objects from several Management Information Bases (MIBs). For more information about these MIBs, see the eHealth SystemEDGE User Guide.

SystemEDGE Self-Monitoring Features

When you manage a large enterprise network with hundreds of systems, you may need to place limits on the information and number of systems that your agents are monitoring, and on the poll rate. The unique self-monitoring capability of the SystemEDGE agent is specifically designed to provide the kind of management by exception that is necessary in distributed network environments.
The SystemEDGE agent can monitor thresholds, processes and Windows services, process groups, log files, and Windows events. SystemEDGE also provides history collection. You can configure these self-monitoring features by adding entries to the monitoring tables of the Systems Management MIB. You can add these entries manually to the sysedge.cf file, or you can use AdvantEDGE View or another element manager to edit the sysedge.mon file with SNMP Sets. For instructions, see the eHealth SystemEDGE User Guide and the eHealth Help.

How You Can View System Data and Manage SystemEDGE Agents

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

You can use AdvantEDGE View to do the following:

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

To access AdvantEDGE View on the eHealth Web user interface

1. Log In to the eHealth Web User Interface.
2. Select the Systems & Apps tab, and then click AdvantEDGE View.
   The AdvantEDGE View page appears.

Important! If you cannot access the Systems & Apps tab, you may not have the correct license or permissions. Use the Administration tab to set your permissions. For more information, see the eHealth Help.

To use AdvantEDGE View, see the eHealth Help for instructions.

Discover System Elements

Before you can run reports with eHealth, you must identify the system elements in your enterprise. You can either use the eHealth discover process to identify system elements, or you can import the system information using the DataSync database configuration information (DCI) import process.
When you run the eHealth discover process for system elements, eHealth searches the specified IP addresses for systems. When eHealth discovers a system, it creates a system element and the following:

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

eHealth creates process elements and process set elements for a system if the system has a SystemEDGE or NSM agent and if the application that is running on that system is defined in the process definition file.

**Collect Data from System Elements**

When you run the discover process and select System as the technology, eHealth searches the specified IP addresses for systems. If you also select Use Process Sets, you can track the impact of individual processes for the applications that are running on the system.

**To discover system elements**

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth server.
2. Create a Discover Policy based on the System technology, and select the Use Process Sets checkbox.
3. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
   
   The Discover window appears.
4. Select the specific IP addresses to use or another method of discovery.
5. Select the policy name.
6. In the Community Strings field, specify one or more community strings that allow read-write or read-only permission to the applications.
7. Click Discover. (For detailed instructions about running the Discover process, see Chapter 3: Discovering Resources.)

**Schedule Configuration Update for System Elements**

After you identify the system elements, you need to collect performance data from them on a regular basis. You can create a scheduled job to collect data automatically through the eHealth poller, and you can import data using the DataSync database data information (DDI) tools. For more information about using DataSync, see the eHealth Data Integration Guide.
To schedule a discover job for system elements, follow these steps:

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to manage discoveries. The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, Resource Discovery, Policies.
3. Create a Discover Policy based on the System technology, and select the Use Process Sets option.
4. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover. The Discover window opens.
5. In the Discover window, specify the IP addresses that discover should search, select the Discover Policy, and specify community strings that allow read-write or read-only permission to the system elements.
6. Select the Schedule tab and specify the days and times.
7. Click Schedule New Job.

View Unlicensed SystemEDGE Agents

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

To view a list of the unlicensed agents

1. On the eHealth console, select Setup, Poller Configuration. The Poller Configuration dialog appears.
2. Select Unlicensed SysEdge Element in the List Elements of Type field, and click Refresh Element List. You can rediscover these elements after you license them through AdvantEDGE View. When they are licensed, eHealth can begin to poll them.

System Process Set Configuration

If you have an eHealth – System license, and the SystemEDGE agent or NSM agent is installed and licensed on your systems, you can create process sets, which are collections of one or more processes that relate to a specific application. eHealth can monitor process sets to report on the applications and processes that are running on those systems.

It is important to monitor the effect of an application and its processes to determine whether a system can support the application effectively. If a system cannot support the application, users experience delays and problems while using the application.
Most systems track the impact of individual processes in the system. To monitor the impact of all processes that relate to an application, you must associate them with the application. eHealth uses a process definition to associate processes that you want to monitor as an application. It also identifies the process sets to discover. After polling the processes, eHealth then aggregates the data into the associated process set. To successfully monitor the processes, you must discover the system using a community string that has read-write permissions.

**Process Set Usage**

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

eHealth allows you to define various process sets to identify all processes that are running on your system and to monitor problems that occur with a particular application. As applications change or become obsolete, you should redefine, delete, or rename the process sets as necessary.

For example, you may want to define a process set to determine how your e-mail application’s processes affect the CPU utilization of your mail server and its clients. When you later upgrade your e-mail application to the next release, you can modify the process set definition so that eHealth creates an element for the processes contained in the new release.

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

**Use Discover Rules to Discover Process Sets**

eHealth uses discover rules when it attempts to discover a process set. It adds a particular set of eHealth elements to your database during the discover process based on the discover rule that you specify in the Create Process Set window. By default, eHealth uses a default discover rule named Create Always. The discover process creates elements for all processes that you include in the process definition for that process set, regardless of whether a given process is actually running.
You can accept the default discover rule, or you can do one of the following:

- Select Create if Key Process is Found. eHealth creates elements for the process set and all of its processes only if it finds the key process. The key process is a unique and persistent process for the application.
- Select Create if Found. eHealth creates elements for those processes that it finds. Discover finds a process only if it is actually running.
- Select Create if Key Process and Found. If eHealth finds the key process, it creates elements for the key process and only those processes that are running.


By default, eHealth does not store the polled statistics data for individual process elements in the database. To report on individual process elements, you must add the System - Store Process Statistics discover parameter to your Discover Policy before discovering those elements and set its value to yes. (The default value is no.)

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

Process sets do consume a poller license. To obtain a list of all elements in your database and to determine whether they require licenses, use the nhListElementLicenses command. For instructions on using this command, see the *eHealth Commands and Environment Variables Reference Guide*.

**Create a Process Set for an Application**

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

**To create a process set for an application**

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth server.
2. In the left pane, select Tasks and Information, Resource Discovery, Process Sets, and then right-click and select New Process Set. The Create Process Set window appears.
3. Specify the name and define the version of the application that you want to monitor.

**Note:** The Process Set Version field is a descriptive field. eHealth does not validate your entry.
4. Click OK. The New Process Set dialog closes. In the Process Definition Editor dialog, eHealth highlights the new process set in the Process Set list and displays the name in the Process Set field, but it does not display any process names in the Name field below it.

5. (Optional) Exclude all processes from eHealth’s calculation for total CPU utilization.

6. Accept the default discover rule, Create Always, or select another rule from the Discover Rule list.

7. Click OK.

The name of the new process set appears under Process Sets in the left pane.

8. Right-click the process set name and select New Process.

The New Process window appears.

9. Specify the name of a process. This name must be the actual string for which the discover process searches. You must specify it exactly as it appears in the system’s process list. (You can view this information from an AdvantEDGE View Process Information query. For more information, see the eHealth Help.)

10. Specify the matching method that eHealth should use during the discover process. Do one of the following:

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

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

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

12. (Optional) If the process is a unique and persistent process for the application, select Key Process. If eHealth finds this process during the discover process, it creates elements for all processes in the process set.

13. (Optional) If you do not want eHealth to include a process when determining a process set’s availability, deselect Mandatory Process.

14. Specify the operating system on which the process can run.

15. Click OK.

16. Create more processes by repeating Steps 9 through 16.
Delete Processes from a Process Set Definition

You can delete a process definition from a process set. You can also remove all existing process definitions and add new processes to the set. To do so, you must delete the process set definition from the file on disk, and then recreate it.

To delete a process definition from the process set definition

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth server.
2. In the left pane, select Tasks and Information, Resource Discovery, Process Sets.
   eHealth displays all existing process sets.
3. In the left pane, select the process set that contains the process.
   The processes contained in that process set appear in the right window.
4. Right-click the process name and select Delete Process.
   A confirmation window appears.
5. At the prompt, click Yes.
   eHealth deletes the process definition from the process file on disk.

Delete a Process Set Definition

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

To delete a process set definition

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth server.
2. In the left pane, select Tasks and Information, Resource Discovery, Process Sets.
   eHealth displays all existing process sets in the right window.
3. Right-click the process set name and select Delete Process Set.
   A confirmation window appears.
4. At the prompt, click Yes.
   eHealth deletes the process set definition from the file on disk.

Example: Create a Process Set

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

1. Access the OneClickEH Console as a web user who has permission to perform discoveries, and then log in to your eHealth server.
2. In the left pane, select Tasks and Information, Resource Discovery, Process Sets, and then right-click and select New Process Set.
   The Create Process Set window appears.
3. Specify ehealth as the name and specify 6.1 as the version of the application that you want to monitor.
   **Note:** The Process Set Version field is a descriptive field. eHealth does not validate your entry.
4. (Optional) Exclude all processes from eHealth’s calculation for total CPU utilization.
5. From the Discover Rule list, select Create If Key Process Is Found.
6. Click OK.
   The name of the new process set appears under Process Sets in the left pane.
7. Right-click the process set name and select New Process.
   The Process window appears.
8. Add the key process first by doing the following:
   a. Specify nhiServer in the Name field.
   b. Accept Full Name as the matching method (the default).
   c. Select Key Process to define this process as a unique and persistent process for this application.
   d. Accept Mandatory Process (the default) to include this process when determining this process set’s availability.
   e. Accept any from the Operating System list (the default).
   f. Click OK.
   g. Click New next to the process list to display the New Process dialog.
9. Add the second process by doing the following:
   a. Right-click the process set name and select New Process.
   a. Specify nhiDbServer in the Name field.
   b. Accept Full Name as the matching method (the default).
   c. Accept Mandatory Process (the default) to include this process when determining this process set’s availability.
   d. Accept any from the Operating System list (the default).
   e. Click OK.
10. Add the third process by doing the following:
    a. Right-click the process set name and select New Process.
    b. Specify nhiConsole in the Name field.
    c. Accept Full Name as the matching method (the default).
    d. Accept Mandatory Process (the default) to include this process when determining this process set’s availability.
    e. Accept any from the Operating System list (the default).
f. Click OK.

g. In the Process Definition Editor dialog, select New next to the process list to display the New Process dialog.

11. Add the fourth process by doing the following:
   a. Right-click the process set name and select New Process.
   b. Specify \texttt{nhiLiveExSvr} in the Name field.
   c. Accept Full Name as the matching method (the default).
   d. Accept Mandatory Process (the default) to include this process when determining this process set’s availability.
   e. Select any from the Operating System list.
   f. Click OK.
   g. In the Process Definition Editor dialog, select New next to the process list to display the New Process dialog.

12. Add the fifth process by doing the following:
   a. Right-click the process set name and select New Process.
   b. Specify \texttt{nhiPoller} in the Name field.
   c. Accept Full Name as the matching method (the default).
   d. Specify -live in the Arguments field. This argument instructs your system to monitor the Live Trend poller.
   e. Accept Mandatory Process (the default) to include this process when determining this process set’s availability.
   f. Accept any from the Operating System list (the default).
   g. Click OK.

**Sample Reports for Process Sets**

After you create process sets, you can use eHealth to run At-a-Glance, Trend, Top N, What-If, and MyHealth reports for your process sets. For example, you can run an At-a-Glance report for a System Process Set and use the CPU Utilization by Process Set chart to determine the CPU utilization for each process group that you have created. You can compare the utilization trends to see which process set consumed the most CPU processing resources over the report period.

When you click this chart, eHealth displays the All Process Sets – CPU Utilization by Process Set chart, which you can use to compare when and how much each process set utilizes the CPU resources of the system. This information can help you to determine whether a process set is overloading the CPU resources so that you can consider relocating applications to other systems to improve system and application performance.
How to Resolve System Polling Errors

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

To replace the community string for defined process sets, follow this process:
1. Access the OneClickEH Console as a web user who has permission to edit elements, and then log in to your eHealth server.
2. In the left pane, select Tasks and Information, Polling Management, All Errors.
3. Double-click the element to display the Edit Element window.
4. Select the General tab, specify a read-write community string, and click OK.

Resolve Excessive Use of Disk Space by SystemEDGE Log Files

As eHealth polls the eHealth elements that support the SystemEDGE agent and eHealth AIMS, the SystemEDGE agent writes information and warning messages to the sysedge.log file (for Windows) or the syslog facility (on UNIX), by default. You may want to limit the size of these files to conserve disk space. For instructions on limiting the file size, see the eHealth SystemEDGE User Guide.

eHealth Reports for Systems

eHealth reporting helps you to assess performance, locate faults, and diagnose problems on hardware devices. The Unicenter NSM system agent delivers granular data so that reports display even momentary changes. The agents report performance statistics related to CPU, storage (disk and partition), memory (physical and virtual), communications, processes, and systems. These statistics are used in eHealth reports. Because the Unicenter NSM system agent has short sampling intervals, even sudden spikes in performance will appear in your reports. You can generate system reports, process set reports, and perform Live Health monitoring.

These reports can help you track the performance of groups of elements and look for situations that might require attention. They can also help you summarize performance by enterprise, region, department, or business unit.

After you identify the system elements that you want to manage, you can use eHealth to generate the following types of reports for systems:
- At-a-Glance
- Trend
You can also purchase additional licenses to run the following types of eHealth reports:

- Health reports
- Service Level reports

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

**Important!** You can create custom variables and then build custom reports on those variables if you have purchased the eHealth Custom Variable product and you have an eHealth Report Developer license. For more information, see the eHealth Customizing Variables Administration Guide and the eHealth Report Designer Reference Guide.

**To run eHealth reports**

1. **Log In to the eHealth Web User Interface** by specifying a user name and password of an administrator who has permission to run reports, and then click OK.
   
   The eHealth Web user interface appears.

2. Select the Run Reports tab.

   The Run Reports page appears.

3. Select a report template from the report list in the left pane.

   The page refreshes, and the selected template appears in the right pane.

4. On the Run Report page, do the following:
   
   a. Specify the criteria for the subject of the report (element, a group, or a group list), and select System under Technology.
   
   b. Specify a time range for the report.
   
   c. (Optional) Specify a time zone.
   
   d. Customize the presentation by clicking More Options and setting presentation attributes.
   
   e. Click Generate Report.

The next sections provide general information about the reports that you can run with eHealth System and Application. For detailed information and sample reports, see the eHealth Reports User and Administration Guide and the eHealth Help for reports.
At-a-Glance Reports for Systems

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

Trend Reports for Systems

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

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

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

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

Top N Reports for Systems

A Top N report can list all elements in a group that exceed or fall below the report criteria goals that you specify. You can also specify the goal for each variable. eHealth calculates the difference between the actual value for that variable and the goal that you have set.

What-If Capacity Trend Reports for Systems

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

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

Health Reports for Systems

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

You can use a Health report to do the following:

- Identify normal and exceptional system behavior.
- Compare the performance of a group of elements during a report period to their performance over a baseline period.
- Detect changes in behavior that indicate that problems are about to happen or are currently happening.
- Identify trends in volume.
- Identify systems that require further investigation.

Health reports are generally several pages long.

Service Level Reports for Systems

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

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

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

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

- **Business Unit**, which summarizes the service level for the system resources that belong to a department, company, or organization.
Process and Process Set Reports

If you are interested in monitoring application performance, you can run process or process set reports to determine if your application is performing well, or if the system is no longer able to support the application. If it is not, you can add resources or upgrade to a more robust system to help the application perform better.

You can also use the Live Health application to define system thresholds and to detect potential outages and delays that can cause downtime and service degradation. There are four profiles relating to Unicenter NSM systems management. System profiles also include some process alarms. You can apply the following profiles to groups of system elements to monitor them for the conditions described.

Using Live Health with the SystemEDGE Agent

If you have a Live Health license and you are using eHealth — System and Application, you can configure the SystemEDGE agent to send traps to your eHealth system so that you can view SystemEDGE traps in the Live Exceptions Browser and manage them with Fault Manager. Live Exceptions provides network operations center (NOC) and systems, application, and network management personnel with real-time alarms condition reporting by identifying problems that include delay, errors, failures, security, or configuration changes. It can display information about alarms in the Live Exceptions Browser, as well as send traps (alarms) to NMSs and other trap destinations.

Live Exceptions includes default profiles for all eHealth technology types. The profiles organize alarm variables by delay, availability, unusual workload, and latency. As a Live Health administrator, you can define alarm conditions by specifying variables to examine, thresholds to detect, and intervals over which to examine the data. You can also clear alarms manually and disable rules within a profile.

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

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

You can edit the sysedge.cf file to configure the SystemEDGE agent to feed specific traps to Fault Manager for your systems and applications. For information about configuring SystemEDGE, see the eHealth SystemEDGE User Guide. For more information about using Fault Manager, see the eHealth Help.
Chapter 11: Managing and Monitoring Applications

This chapter contains the following sections:
- Guidelines for Monitoring Applications
- Application Data Collection
- Run eHealth Reports for Applications

Guidelines for Monitoring Applications

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

To monitor your applications most effectively, you must have the following components:
- eHealth (with Application Insight and AdvantEDGE View licenses)
- SystemEDGE agents (installed on every system that you want to monitor)
- eHealth AIMs (installed with the SystemEDGE agent on the systems that you want to monitor)
- Each system that is running applications you want to monitor requires only one SystemEDGE agent. You can install multiple eHealth AIMs on each system.

To specify license information for the first time, see How to Add eHealth Licenses on page 29.

Collect Application Data

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

1. Install and configure the SystemEDGE agent on the system that you want to monitor. For instructions, see the eHealth SystemEDGE User Guide.

2. On the same system, install and configure the eHealth AIM for the application that you want to monitor. For instructions, see the user guide for the eHealth AIM that you are using.

3. From the OneClick for eHealth console, discover application elements.

4. Run reports on the discovered elements that provide application-specific data.

When you have an Application Insight license, you can run eHealth reports on application service elements, as illustrated in Figure 1. Application service elements represent an application instance that is monitored by an eHealth SystemEDGE agent and an eHealth AIM.

![Diagram of Application Data Collection](image)

**Figure 1** Obtaining Application Data

**Application Data Collection**

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

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

The following table lists the existing eHealth AIMs and the applications for which they provide management.

<table>
<thead>
<tr>
<th>Module</th>
<th>Manages and Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth AIM for Apache</td>
<td>Apache Web server</td>
</tr>
<tr>
<td>eHealth AIM for Check Point FireWall-1</td>
<td>Check Point FireWall-1 application</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft Exchange</td>
<td>All key Microsoft Exchange services, such as the Connectors, Information Store, Exchange Directory, Message Transfer Agent, and more</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft IIS</td>
<td>Microsoft IIS Web server and its services, including World Wide Web (WWW), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP).</td>
</tr>
<tr>
<td>eHealth AIM for Microsoft SQL Server</td>
<td>Microsoft SQL Server databases, including SQL core processes, queries, transaction logs, and backups.</td>
</tr>
<tr>
<td>eHealth AIM for Network Services for UNIX</td>
<td>Vital network services for UNIX systems, including Sendmail, DNS, Lightweight Directory Access Protocol (LDAP), network file system (NFS), Network Information Services (NIS), and Dynamic Host Configuration Protocol (DHCP)</td>
</tr>
<tr>
<td>eHealth AIM for Network Services for Windows</td>
<td>Vital network services for Windows systems, including Active Directory, DHCP, DNS and Windows Internet Naming Service (WINS).</td>
</tr>
<tr>
<td>eHealth AIM for Oracle</td>
<td>Oracle database and application, including configuration information and status of Oracle processes and files.</td>
</tr>
</tbody>
</table>

For more information about these eHealth AIMs and instructions on querying eHealth AIMs for application data, see the user guide for the eHealth AIM that you want to use and the eHealth Help.
Discover Application Elements

After you configure the SystemEDGE agent and eHealth AIMs to collect application data, you can use eHealth to discover applications and to report on them. When you run the discover process and select the Application technology (as described in section on page 190), eHealth searches the list of IP addresses for applications. It finds an application when it locates a system that is running both the SystemEDGE agent and an eHealth AIM. When you discover an application, eHealth creates an application service element and an application service process set element.

eHealth looks for application elements on User Datagram Protocol (UDP) port 1691 by default. You can configure eHealth to search for application elements on other agent ports by modifying the Ports - Application policy parameter. For more information on specifying ports and setting Discover Policy parameters, see How to Discover Resources Interactively on page 39.

To discover application elements

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage discoveries.
   
The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, Resource Discovery, Policies.
3. Create a Discover Policy based on the Application technology.
   
   **Important!** If you do not select both the System and Application technologies, you cannot discover eHealth AIMs.
4. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
5. Specify the IP addresses to use, or select another discover method.
6. Select the Discover Policy.
7. Specify one or more community strings that allow read-write or read-only permission to the application elements.
8. Click Discover. (For detailed instructions for running the Discover process, see Chapter 3: Discovering Resources.)

View Unlicensed eHealth AIMs

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

To view the unlicensed eHealth AIMs

1. On the eHealth console, select Setup, Poller Configuration. The Poller Configuration dialog appears. The unlicensed eHealth AIMs have a suffix of unlicensed.
2. To view only the unlicensed SystemEDGE agents, eHealth AIMs, and Service Availability modules, select Unlicensed SysEdge Element in the List Elements of Type field, and click Refresh Element List. You can rediscover these elements after you license them through AdvantEDGE View or Live Health. When they are licensed, eHealth can begin to poll them.

Schedule Data Collection for Application Elements

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

To schedule a discover job for application elements, follow these steps:

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage scheduled jobs.
   The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, Resource Discovery, Policies.
3. Create a Discover Policy based on the Application and System technologies.
4. In the left pane, select Tasks and Information, Resource Discovery, Interactive Discover.
5. In the Discover window, specify IP addresses, the policy name, and a community string that allows read-write or read-only permission to the application elements.
6. Select the Schedule tab.
7. In the schedule window, specify the days and the time, and specify an e-mail address of any user who would like to review the log file.
8. Click Schedule New Job.

Application Element Naming Conventions

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

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

You can delete application elements using the OneClick for eHealth console.

To delete an application element

1. Access the OneClickEH Console as a web user who has permission to manage elements, and then log in to your eHealth server.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Find the element in the table, right-click, and select Delete.
4. When the confirmation window appears, click Yes.

**Important!** If you delete an application service element, you also delete all process sets that are associated with that element. You must click OK or Apply to save your changes. If you click Cancel, you will lose all work that you have performed.

Create Application Groups

Before you generate Application reports, you might want to organize your application service elements by creating groups. Groups help you manage your elements. Create groups to organize application elements that are related in some way.

To create groups of application service elements

1. Access the OneClickEH Console as a web user who has permission to manage elements and manage groups, and then log in to your eHealth server.
2. In the left pane, select Managed Resources, Elements. The Elements window appears.
3. Filter the list. Include a wildcard such as an asterisk (*) to match characters, or a question mark (?) to match a single character.
4. Select the application service elements that you want to include, and then right-click and select Create Group with Selected Elements. The Create Group window appears.
5. Specify the first group name and a description, and then click OK. The group immediately appears under By Group.

Create Application Group Lists

Before you generate Application reports, you might want to organize your groups of application service elements by creating group lists. A group list is a collection of one or more groups. A group can belong to more than one group list. By creating group lists, you can associate groups that are related in some way.
To create group lists of application groups

1. Access the OneClickEH Console as a web user who has permission to manage elements and manage groups, and then log in to your eHealth system.
2. In the left pane, select Managed Resources.
3. Right-click By Group List and select New Group List.
   The Create Group List window appears.
4. Specify a name and a description.
5. (Optional) Enable the group list to be visible in the Business Service Console (BSC).
6. Click OK.
   The window closes, the console refreshes, and the new group list appears in the left pane under By Group List.
7. Double-click the group list name under By Group List and select the Groups Not in Any Group List tab.
   eHealth displays all groups that are not associated with an existing group.
8. Select the groups of application service elements from the list, right-click, and select Add Selected Groups to Group List.
   eHealth adds the groups to the group list.

Run eHealth Reports for Applications

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

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

To run eHealth reports:

1. Log In to the eHealth Web User Interface by specifying a user name and password of an administrator who has permission to run reports, and then click OK.
   The eHealth Web user interface appears.
2. Select the Run Reports tab.
   The Run Reports page appears.
3. Select a report template from the report list in the left pane.
   The page refreshes, and the selected template appears in the right pane.
4. On the Run Report page, do the following:
   a. Specify the criteria for the subject of the report (element, a group, or a group list), and select App Service under Technology.
   b. Specify a time range for the report.
   c. (Optional) Specify a time zone.
   d. Customize the presentation by clicking More Options and setting presentation attributes.

5. Click Generate Report.

For more information about eHealth reports, see the eHealth Reports User and Administration Guide and the eHealth Help.

At-a-Glance Reports for Applications

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

If you also discovered the systems using the System technology, you can monitor the health and performance of the system and its resources using System At-a-Glance reports in addition to the Application Service At-a-Glance reports.

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

At-a-Glance reports for applications include charts for variables that are specific to the application service you are monitoring. For example:

- If you are running an At-a-Glance report for Apache application service elements, it will include the Number of Apache Processes chart.
- If you are running an At-a-Glance report for Oracle application service elements, it will include a Block Changes per Transaction chart.
- If you are running an At-a-Glance report for Exchange application service elements, it will include a Disk Usage chart.

Trend Reports for Applications

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

**Top N Reports for Applications**

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

**MyHealth Reports for Applications**

You can include charts for application service monitoring in your MyHealth reports. MyHealth provides eHealth Web users with one or more customized reports on the elements and groups that they consider critical. You can run MyHealth reports from the MyHealth tab in the eHealth Web user interface.
Appendix A: The Discover Algorithm

This chapter contains the following chapters:

- eHealth Discover Matching Algorithm
  - How eHealth Matches at the Device Level
  - How eHealth Matches at the Agent Level
  - How eHealth Matches at the Element Level
  - How eHealth Matches Discover Keys
  - How eHealth Matches at the Physical Address Level
  - How eHealth Matches MIB Attributes

**eHealth Discover Matching Algorithm**

Discover is able to resolve an infrastructure change when it can update the database with the information without duplicating an element or incorrectly changing existing information. eHealth uses a complex matching algorithm to identify changes within your infrastructure. The discover process tracks changes and correctly updates the database by matching at the nmsSource level first. It then matches at three abstract levels: device, agent, and element, as illustrated in the following figure:
These methods help the discover process determine whether an element is a new addition or if it is an existing element that has been moved. You must track these changes to maintain the accuracy of eHealth reports. The discover log reports the results of these comparisons so that you can identify the changes that discover made or recommended.

How eHealth Matches at the Device Level

eHealth uses a very complex matching algorithm to identify changes within your infrastructure.

To match at the device level, eHealth follows these steps:

1. Attempts to match all of these attributes:
   - System name – Name assigned to the sysName variable in the MIB on the device.
   - Unique device ID – Typically, a chassis ID or similar attribute found in the MIB. Some devices allow you to override the unique device ID with a chassis ID. These values must be unique across your IT infrastructure.
   - IP address – IP address specified by the user for the discover (for devices, eHealth always uses the polled IP address of the device).

   - If a match on all three attributes or the two-out-of-three match produces multiple possibilities, discover attempts to match the set of interface physical addresses and then the set of interface IP addresses.
   - If none of the devices match at least two of the three attributes, discover attempts to match sets of physical addresses and then sets of IP addresses. If discover does not find any matches through these methods, the device is new.

3. Verifies the device match. After matching attributes, discover compares the set of physical and IP addresses from the device interfaces with those that are stored in the database. The greater the number of matches, the greater the confidence in the device match.
   - If attribute matching indicated that a device is new, lack of an address match improves the confidence that the device is new.
   - If discover does not identify any attribute matches but does identify a near-perfect address set match, the attributes for an existing element have changed significantly. eHealth accepts the address set match (by default) and updates the attributes in the database to match the newly discovered attributes.

How eHealth Matches at the Agent Level

eHealth uses a very complex matching algorithm to identify changes within your infrastructure. Once eHealth finds a matching device, it proceeds to match at the agent level. eHealth sets the agent type in the database by gathering information from the MIB on the device.
To match at the agent level, eHealth does the following:
1. Matches on the MIB translation file (MTF) of the parent element (if it exists).
2. Matches the SNMP port.
3. Matches the enterprise ID.

If an agent does not match at the parent MTF, SNMP port, and enterprise ID, eHealth considers it to be a new agent.

How eHealth Matches at the Element Level

eHealth uses a very complex matching algorithm to identify changes within your infrastructure. Once it finds an agent, eHealth proceeds to match at the element level to track changes and update the database:

To match at the element level, eHealth does the following:
1. Matches the discover keys.
2. Matches the physical address and virtual interface ID (if defined).
3. Matches the MIB indexes and MTF.

Discover Key

eHealth uses a unique key to identify each element during discovery. For most elements, this unique key is the value of the ifDescr field. All interface elements of a device should have unique (that is, within the device) ifDescr values. eHealth creates discover keys for newly discovered elements that meet the following requirements:
- The element is certified for use with eHealth.
- eHealth was able to obtain (from the MIB) the attributes and other information necessary to create a discover key.

How eHealth Matches Discover Keys

eHealth uses a very complex matching algorithm to identify changes within your infrastructure. Once it finds an agent, eHealth proceeds to match at the element level to track changes and update the database. To match at the element level, eHealth first matches discover keys.

To match discover keys, eHealth follows this process:
1. Compares the unique key for each newly discovered element with the unique key for elements that are already in the database:
2. If none of the elements in the database have that unique key, it considers the newly discovered element to be a new element.
3. If the newly discovered element and an element in the database have the same unique key and they have identical information, it considers the newly discovered element to be a *duplicate*.

4. If the newly discovered element and an element in the database have the same unique key, but they have different information, it considers the newly discovered element to be an *updated* element.

**Discover Key Formats**

eHealth uses information that it obtains from the MIB to create and maintain discover keys for component elements in the database. For interfaces, the discover key also includes a component type that eHealth assigns based on discovered information. All discover keys include different fields that are based on the type of element. The following table lists the types of components for which eHealth can create discover keys and describes their format.

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Discover Key Format</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application service</td>
<td><em>applicationName</em></td>
<td>Specifies the name of the eHealth AIM.</td>
</tr>
<tr>
<td>Application service process sets</td>
<td><em>applicationName</em></td>
<td></td>
</tr>
</tbody>
</table>
| Ascend, Cisco, and Shiva ISDN interfaces | ras *componentType* ifDescr | *componentType* specifies the type that eHealth specifies based on information about the element that it obtains from the MIB.*  
*ifDescr* specifies the value of the ifDescr variable in the MIB. |
| Ascend, Cisco, and Shiva modem interfaces | pool *componentType* ifDescr | *componentType* specifies the type that eHealth specifies based on information about the element that it obtains from the MIB.*  
*ifDescr* specifies the value of the ifDescr variable in the MIB. |
| ATM path on a Cisco LightStream 1010 switch | ifDescr VPI | *ifDescr* specifies the value of the ifDescr variable in the MIB.  
*VPI* specifies its Virtual Path Identifier. |
### eHealth Discover Matching Algorithm

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Discover Key Format</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| ATM channel on a Cisco LightStream 1010 switch | ifDescr VPI VCI | - *ifDescr* specifies the value of the ifDescr variable in the MIB.  
- *VPI* specifies its Virtual Path Identifier.  
- *VCI* specifies its Virtual Channel Identifier. |
| Bay Networks, WellFleet, and generic Frame Relay permanent virtual circuits (PVCs); other PVCs conforming to RFC 1604 | ifDescr DLCI | - *ifDescr* specifies the value of the ifDescr variable in the MIB.  
- *DLCI* specifies its Data Link Connection Identifier (DLCI), the number assigned by the Frame Relay station to a specific data link connection. |
| Cisco Catalyst 5000 Switching System interfaces | port Module-module#-Port-port# | - *portModule-module#* specifies the interface’s module number as one of the following: 5500, 5000, 5002.  
- *Port-port#* specifies the interface’s port number. |
| Generic router and system interfaces | componentType ifDescr | - *componentType* specifies the type that eHealth specifies based on information about the element that it obtains from the MIB.**  
- *ifDescr* specifies the value of the ifDescr variable in the MIB. |
| Physical disks on systems | deviceName | Specifies the disk device name, as obtained from the MIB. |
| Processes | processSetName | Specifies the names that you specify in the Process Definition Editor dialog. Arguments are optional. |
| Process sets | processSetName - arguments |  |
How eHealth Matches at the Physical Address Level

eHealth uses a very complex matching algorithm to identify changes within your infrastructure. Once it finds an agent, eHealth proceeds to match at the element level to track changes and update the database. To match at the element level, eHealth first matches discover keys and then matches physical addresses.

To match at the physical address level, eHealth compares the physical address (ipPhysAddr) of the elements with those that are stored in the database. In cases of virtual interfaces, such as Frame Relay PVCs, ATM PVCs, or workgroup hub modules (where the physical interface can be the same for more than one interface), discover uses the virtual channel identifier to identify virtual addresses within a physical one.
How eHealth Matches MIB Attributes

eHealth compares MIB attributes of elements to identify components for which it cannot create a discover key and to distinguish among two or more component elements that have identical discover keys. To match MIB attributes, eHealth compares the MIB attributes of discovered elements to values in the database to determine whether the discovered elements are new. However, identifying components by comparing MIB attributes can be unreliable because the comparison includes SNMP indexes, which can shift when the device is restarted. The discover process cannot determine whether the SNMP indexes shifted. If MIB indexes are the only differentiating factor among elements (that is, the discover keys are not unique, and the physical address is not unique or is undefined), discover cannot accurately track any index shifting that may occur.
Appendix B: eHealth Element Naming Conventions

This appendix includes the following topics:
- LAN/WAN Element Discovery
- Router/Switch Element Discovery
- Traffic Accountant Element Discovery
- System Element Discovery
- Application Element Discovery
- Modem Pool and RAS Element Discovery
- Response Element Discovery
- QoS Element Discovery

LAN/WAN Element Discovery

When you run the discover process and select the LAN/WAN technology, eHealth searches the specified IP addresses for interfaces. Upon discovering an interface, eHealth does the following:
- For each Ethernet, 802.3, token ring, or FDDI type interface, it creates a LAN element.
- For each of the following, it creates a LAN or WAN element and identifies the type of interface, as well as one or more SNMP indexes assigned to it:
  - LAN or WAN interface
  - ATM port, path, and channel
  - Frame Relay PVC

eHealth defines WAN links—including those used for ATM or to carry Frame Relay PVCs—as WAN elements. You can poll and report on ATM ports, paths, and channels, and Frame Relay PVCs.
Router/Switch Element Discovery

When you run the discover process and select the Router technology, eHealth searches the specified IP addresses for routers and switches. You can use either standard router/switch reporting or enhanced router/switch reporting. The default mode of the router/switch discover process is enhanced. If a device does not support enhanced switch reporting, eHealth discovers the switch as a traditional (standard) switch. For a list of devices that support enhanced router/switch reporting, see the Certified Devices Web page at http://support.concord.com.

With standard router/switch reporting, for each router or switch, eHealth creates a router/switch element and the following:

- Interface element for each interface on the router/switch
- CPU element for each CPU on the router/switch

  The default element name for a CPU or interface element includes the name of the router/switch to which it belongs. Although the discover process creates an element for each interface on a router/switch, eHealth router reports do not report the statistics for the individual interfaces.

  Instead, the reports combine the statistics for the interface elements. For example, router reports show the following:

- Average line utilization as a percentage of total line capacity
- Percentage of all frames with faults and frames that were discarded

  eHealth summarizes the data from the interfaces to determine the amount and type of traffic that passed through the router or switch. It also analyzes the CPU utilization and buffering to measure the health of your routers or switches.

If you run the discover process for router/switch elements after running it for LAN/WAN elements, the database uses the existing LAN element entry for the same router/switch LAN interface element and the existing WAN element entry for the same router/switch WAN interface element. If you rediscover the router/switch interface elements first, you can rediscover them using the LAN/WAN technology to report on the individual elements.

Enhanced Router/Switch Reporting

With enhanced router/switch reporting, eHealth does the following:

- If the router/switch is a supported switch Plus device, eHealth creates the router/switch element and the following:
  - Interface element for each interface on the router/switch
  - CPU element for each CPU on the router/switch
  - Backplane element
- If the switch is a supported switch Lite device, eHealth creates the router/switch element and the following:
  - CPU element for each CPU on the router/switch
  - Backplane element
eHealth uses the router/switch CPU element to store CPU utilization, as well as memory and environmental statistics. Therefore, the discover process always creates a CPU element for a Plus or Lite router/switch, regardless of whether the CPU utilization data is available from the router/switch. The default mode of the router/switch discover process is switch Plus. If eHealth discovers a router/switch that is a supported Plus device, it creates the router/switch element, its interfaces, the backplane, and the CPU. If you rediscover a traditional router/switch, eHealth simply adds the backplane and CPU elements.

To discover devices as Lite routers/switches, you must set the value of the Switch Mode Discovery policy parameter to lite. If eHealth discovers a switch that is a supported Lite device, it creates the switch element, the backplane, and the CPU. To change from switch Lite mode to switch Plus mode, you must change the value to plus. However, before rediscovering a Lite switch as a Plus switch, you must first delete it from your database.

**Important!** If you do not delete the Lite switch from the database before rediscovering it, eHealth includes the Lite backplane by aggregating the statistics from the interfaces and the backplane, which results in inflated total statistics for the switch. For the same reason, you must delete an existing traditional or Plus switch element before rediscovering it as a Lite switch.

If a device does not support enhanced switch reporting, eHealth discovers the switch as a traditional switch, including the switch element and its interfaces. In some cases, eHealth discovers a switch as a router when it has been enhanced to include additional router information (for example, a Cisco Catalyst switch with the Router Switch Module (RSM)). For a list of enhanced switch devices, see the Certified Devices Web page at http://support.concord.com.

**LAN/WAN and Router/Switch Element Discovery**

When you choose to concurrently discover LAN/WAN and router/switch elements, eHealth uses essentially the same element naming conventions with the exception of the following:

- When you discover LAN/WAN interface elements using the Router/Switch technology, the router will be the parent for the interface elements.
- When you discover router interfaces using the LAN/WAN technology, the Include detailed data option will be enabled for those elements in the Modify Element dialog.

  eHealth appends -RH to the element name to designate router/switch parents, and the subelements such as CPUs and backplanes. These elements often use the convention `parentName-cpu-x` or `parentName-Bkpln`.

**Traffic Accountant Element Discovery**

When you run a discover process and select the Probes technology, eHealth searches the IP addresses specified for probes. A probe is a device that contains remote network monitoring (RMON) software to record information about the
network traffic that it observes. A probe can also be embedded RMON software in a device. Probes collect data about the conversations between node pairs on the network. Although the information collected by each probe can vary, typical information includes the address of the sending node, the address of the receiving node, the number of packets and bytes transmitted, and the protocol or application type of the data. For information about discovering Traffic Accountant elements, see the eHealth Help.

**System Element Discovery**

When you run the discover process and select the System technology, eHealth searches the specified IP addresses for systems. An additional discover option, Find Processes (Specify write community), is selected by default to track the impact of individual processes in the system. Click Define to define process sets that associate processes as an application. For information about discovering system elements and defining process sets, see the eHealth Help.

When you select the System technology, you can select Find Processes to track the impact of individual processes in the system. Click Define to define process sets that associate processes as an application. For information about defining process sets, see Chapter 10: Managing and Monitoring Systems.

**Application Element Discovery**

When you run the discover process and select the Application technology, eHealth searches the specified IP addresses for applications.

When you discover both system and application elements, eHealth discovers both licensed and unlicensed eHealth application insight modules (AIMs). When you discover response elements, eHealth discovers both licensed and unlicensed eHealth Service Availability (SA) modules. If you have licensed Fault Manager, you can view the unlicensed modules (with a suffix of unlicensed) in the Poller Configuration dialog. To view only the unlicensed system agents, SA modules, and eHealth AIMs, select Unlicensed SysEdge Element in the List Elements of Type field of the Poller Configuration dialog, and then click Refresh Element List. You can rediscover these elements after you license them by using the Systems & Apps tab of the eHealth Web user interface. When they are licensed, eHealth can begin to poll them. For information about licensing these eHealth AIMs, see the eHealth Help.
Modem Pool and RAS Element Discovery

You can run the discover process for modems, modem pools, and Remote Access Server (RAS) devices. You can discover RAS devices as RAS elements, modem pool elements, or both.

- To manage RAS devices as physical devices, discover the devices using the Remote Access Server technology. This enables you to run reports on the RAS device, its CPU, and all of its modems and ISDN interfaces.

- To manage the modems and ISDN interfaces as groups within one or more RAS devices, discover the RAS devices using the Modem Pool technology. This enables you to report on modem pools that might span one or more RAS devices.

If you discover a RAS device using both the Remote Access Server and Modem Pool technologies, eHealth polls the elements on the RAS device twice, once for RAS statistics and once for modem pool statistics. For best poller performance, you should manage RAS devices as RAS elements or modem pool elements, but not both.

When you run a discover process and select the Remote Access Server technology, eHealth searches the specified IP addresses for RAS devices. When eHealth discovers a RAS device, it creates an element for each of the following:

- The RAS
- Each CPU in the RAS
- Each modem in the RAS
- Each ISDN interface in the RAS

eHealth assigns each CPU, modem, and ISDN element to the RAS element to which it belongs. When you run reports for the RAS device, eHealth combines the total data collected for each modem and ISDN element in the RAS to report on the health of the RAS. You can also run reports on the individual modem and ISDN elements in the RAS.

**Important!** Because RAS devices perform routing services, the discover process for routers could discover RAS devices as router elements. If you discover a RAS as a router element, eHealth includes the RAS in router reports, but not in remote access reports. Manage your RAS devices using the Remote Access technology—not Router/Switch technology. If you choose to report on a RAS as both a router element and a RAS element, eHealth polls the RAS device and its elements twice.

When you run a discover process and select the Modem Pool technology, eHealth searches the specified IP addresses for RAS devices.

When eHealth discovers a RAS device, it creates an element for each of the following:

- Each modem pool configured at the device
- Each modem in the device
- Each ISDN interface in the device
If the RAS device agent has modem pool information defined in the MIB, eHealth uses the MIB information to configure the modem pool element name and assign modem and ISDN elements to the modem pool. If the RAS device agent does not have a modem pool definition, eHealth creates a single modem pool element for the RAS device and assigns all modem and ISDN elements in the device to it. If the default modem pool does not reflect your modem pool configuration, you can create modem pool elements and assign the modem and ISDN elements to the correct modem pools, as described in Chapter 4: Maintaining Your Element Configuration.

When you run reports for the modem pool, eHealth combines the total data collected for each modem and ISDN element in the pool to report on the health of the modem pool. You can also run reports on the individual modem and ISDN elements in the modem pool.

Response Element Discovery

When you run the discover process and select the Response Elements technology, discover searches the specified IP addresses for response agents in your network such as Cisco IP SLA and Juniper RPM routers. eHealth can measure the response time of the applications and services that reside on those devices. Response time is the elapsed time between a user request and a system response. By measuring the actual response times that end users experience, you can detect degrading performance and declining availability of your critical services and applications and maintain service levels.

After you discover response elements and save them to the eHealth database, you must create response destination elements. You can create these elements from existing response source elements, or you can specify the IP address of a new element that does not yet exist in the database. You use a destination element to indicate one endpoint of a response path that eHealth monitors. You specify an existing response source to identify the other endpoint of the response path. eHealth monitors activity between the endpoints that you specify. For detailed information about the response technology, see the Using eHealth – Response Administration Guide.

QoS Element Discovery

Quality of Service (QoS) is a technology that allows you to configure different levels of service for different types of traffic in your infrastructure. If you have devices that support QoS, you can configure your routers to recognize different types of traffic, and to treat each type differently based on a Class of Service (CoS) that you define for each traffic type. To implement QoS in your infrastructure, you must identify and define your various types of traffic and configure a CoS for each type. For detailed information about the QoS technology, see the eHealth Help. For instructions on discovering QoS elements, see the Managing Cisco QoS Using eHealth focus topic.
How eHealth Names Elements

After discovering an element, eHealth assigns a name to it. Element names are represented as case-sensitive, but eHealth does not use case to determine the uniqueness of an element. By default, it uses the following format to name elements, as defined in the following table:

devName-suffixMode-suffixType-suffixIndex1-suffixIndex2

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devName</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>suffixMode</td>
<td>For router and system elements only, indicates the type of parent:</td>
</tr>
<tr>
<td></td>
<td>- POOL for modem and ISDN pools</td>
</tr>
<tr>
<td></td>
<td>- RH for routers</td>
</tr>
<tr>
<td></td>
<td>- RAS for remote access servers</td>
</tr>
<tr>
<td></td>
<td>- SH for systems</td>
</tr>
<tr>
<td></td>
<td>- RS for response sources</td>
</tr>
<tr>
<td></td>
<td>- RD for response destinations</td>
</tr>
<tr>
<td></td>
<td>- AP for application paths</td>
</tr>
<tr>
<td></td>
<td>- AH for applications</td>
</tr>
<tr>
<td></td>
<td>- QOS for QoS</td>
</tr>
<tr>
<td>suffixIndex1</td>
<td>The first index from the interface table for the element. System partitions use the partition name (not the index number).</td>
</tr>
<tr>
<td>suffixIndex2</td>
<td>The second index from the interface table for the element.</td>
</tr>
<tr>
<td>suffixType</td>
<td>Indicates the type of element, for example:</td>
</tr>
<tr>
<td></td>
<td>- Apache for Apache application elements (for system agents with appropriate eHealth AIM)</td>
</tr>
<tr>
<td></td>
<td>- atm-path for ATM paths</td>
</tr>
<tr>
<td></td>
<td>- atm-port for WAN ports used for ATM</td>
</tr>
<tr>
<td></td>
<td>- Cpu for CPUs in routers and systems</td>
</tr>
<tr>
<td></td>
<td>- DEP for a generic event source that represents dependency</td>
</tr>
<tr>
<td></td>
<td>- disk for system disk elements (system partition elements do not use this variable)</td>
</tr>
<tr>
<td></td>
<td>- dlcI for endpoints of a Frame Relay PVC</td>
</tr>
<tr>
<td></td>
<td>- enet-port for Ethernet LAN and MIB2 elements</td>
</tr>
<tr>
<td></td>
<td>- Exchange (for system agents with eHealth AIM for Microsoft Exchange)</td>
</tr>
<tr>
<td></td>
<td>- IIS for Microsoft IIS application elements (for system agents with eHealth AIM for Microsoft IIS)</td>
</tr>
</tbody>
</table>
The following table lists the Discover Policy parameters that define the name selection process that the discover process uses to create the `devName` value.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suffixType (continued)</td>
<td>Indicates the type of element, for example:</td>
</tr>
<tr>
<td></td>
<td>- isdn for ISDN devices</td>
</tr>
<tr>
<td></td>
<td>- link for WAN links, including those used for Frame Relay</td>
</tr>
<tr>
<td></td>
<td>- modem for modems</td>
</tr>
<tr>
<td></td>
<td>- OracleDB for Oracle application elements (for system agents with eHealth AIM for Oracle)</td>
</tr>
<tr>
<td></td>
<td>- NetworkSvcs_ServiceName for Network Services for UNIX application elements (for system agents with eHealth AIM for Network Services for UNIX)</td>
</tr>
<tr>
<td></td>
<td>- NetworkSvcsNT_ServiceName for Network Services for Windows application elements (for system agents with eHealth AIM for Network Services for Windows) probe for RMON probe elements</td>
</tr>
<tr>
<td></td>
<td>- rptGroup for repeater groups</td>
</tr>
<tr>
<td></td>
<td>- RD for response destination elements (for system agents with eHealth Service Availability)</td>
</tr>
<tr>
<td></td>
<td>- RS for response source elements (for system agents with eHealth Service Availability)</td>
</tr>
<tr>
<td></td>
<td>- seg for Ethernet LAN RMON elements</td>
</tr>
<tr>
<td></td>
<td>- SONET for fiber-optic cable elements</td>
</tr>
<tr>
<td></td>
<td>- SQLServer for Microsoft SQL application elements (for system agents with eHealth AIM for Microsoft SQL Server)</td>
</tr>
<tr>
<td></td>
<td>- tr for token ring LAN elements</td>
</tr>
<tr>
<td></td>
<td>- unlicensed for unlicensed system agents, Service Availability modules, and eHealth AIMS</td>
</tr>
</tbody>
</table>

The following table lists the Discover Policy parameters that define the name selection process that the discover process uses to create the `devName` value.

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naming - Use DNS</td>
<td>Specifies whether the discover process uses the name provided through the domain name system (DNS) or the content of the sysName field.</td>
</tr>
<tr>
<td></td>
<td>- When set to <em>no</em> (the default), discover uses the sysName field.</td>
</tr>
<tr>
<td></td>
<td>- When set to <em>yes</em>, discover uses the name provided through DNS. However, router parent elements do not use the DNS name or the name specified in the <code>/etc/hosts</code> file regardless of the variable setting.</td>
</tr>
<tr>
<td></td>
<td>- When set to <em>file</em>, discover uses the <em>hosts</em> file defined by an internal variable, <code>NH_HOST_FILE</code>.</td>
</tr>
</tbody>
</table>
The values of the DNS Lookup by ifIpAddress and Naming - Use DNS Discover Policy parameters control how discover selects element names. For each of the four combinations of parameter settings, the discover process uses the first address or name that it finds by following the steps listed in the following table.

<table>
<thead>
<tr>
<th>Discover Policy Parameter Settings</th>
<th>Name Selection Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Lookup by ifIpAddress=yes</td>
<td>1. Use sysName.</td>
</tr>
<tr>
<td>Naming - Use DNS=no</td>
<td>2. Use IP address of the interface.</td>
</tr>
<tr>
<td></td>
<td>3. Use IP address of the device polled address.</td>
</tr>
<tr>
<td>DNS Lookup by ifIpAddress=no</td>
<td>1. Use DNS name of the device polled address.</td>
</tr>
<tr>
<td>Naming - Use DNS=yes</td>
<td>2. Use sysName.</td>
</tr>
<tr>
<td></td>
<td>3. Use IP address of the device polled address.</td>
</tr>
<tr>
<td>DNS Lookup by ifIpAddress=yes</td>
<td>1. Use DNS name of the interface address.</td>
</tr>
<tr>
<td>Naming - Use DNS=yes</td>
<td>2. Use DNS name of the device polled address.</td>
</tr>
<tr>
<td></td>
<td>3. Use sysName.</td>
</tr>
<tr>
<td></td>
<td>4. Use IP address of the interface.</td>
</tr>
<tr>
<td></td>
<td>5. Use IP address of the device polled address.</td>
</tr>
<tr>
<td>DNS Lookup by ifIpAddress=no</td>
<td>1. Use sysName.</td>
</tr>
<tr>
<td>Naming - Use DNS=no</td>
<td>2. Use IP address of the device polled address.</td>
</tr>
</tbody>
</table>

The default setting for the Naming - Truncate by Regular Expression Discover Policy parameter causes the discover process to truncate the name or address at the first period in the name. For example, if the DNS name is red.blue.com, the discover process uses the name red and appends the appropriate element-specific information; an Ethernet interface on this device would be named red-enet-port-1. You can set the Naming - Truncate by Regular Expression Discover Policy parameter to use alternate naming conventions.
For example, if devices have the following names, the default naming conventions use Boston and NY as the main element names, followed by the element-specific information:

Boston.sales.company.com
Boston.eng.company.com
NY.marketing.company.com

Instead, you might prefer element names that distinguish Boston.sales elements from the Boston.eng elements; to do so, use one of these values:

- UNIX: "/.company/.com"
- Windows: \.company\.com

This value truncates the .company.com string from each name. For instructions on setting environment variables, see the eHealth Help.

### How to Customize Element Names

eHealth uses the Naming - Use Alternate Name Scheme Discover Policy parameter to identify a tool command language (Tcl) script that can name discovered elements. You can use this variable with those three variables.

To use the Naming - Use Alternate Name Scheme Discover Policy parameter, edit the nethealthrc.sh file to add the following line, where filename is the full pathname for the Tcl script:

```
export Naming - Use Alternate Name Scheme; Naming - Use Alternate Name Scheme="filename"
```

In a Tcl script, you can use, replace, or expand any of the default variables with the variables listed in the following table. eHealth supplies and understands these variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipAddr</td>
<td>IP address by which the element is discovered.</td>
</tr>
<tr>
<td>community</td>
<td>Community string of the SNMP agent.</td>
</tr>
<tr>
<td>mtfFile</td>
<td>Name of the MTF for the element; if a WAN or Frame Relay element, it is the MTF for the IN element.</td>
</tr>
<tr>
<td>mtfFile2</td>
<td>The MTF for a WAN or Frame Relay OUT element.</td>
</tr>
<tr>
<td>index</td>
<td>Contents of the Index field.</td>
</tr>
<tr>
<td>index2</td>
<td>Contents of the Index 2 field.</td>
</tr>
<tr>
<td>index3</td>
<td>Contents of the Index 3 field.</td>
</tr>
</tbody>
</table>
In addition to the eHealth-specific variables, you can also use these two global variables, which you can access with the global varName statement:

- **env** – The array of available environment variables.
- **Session** – The SNMP session handle needed to make SNMP calls.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>modDescr</code></td>
<td>For Cisco elements only, contents of the ifDescr field are processed. With Cisco elements, this variable is appended to the devName variable before any other variable.</td>
</tr>
<tr>
<td><code>suffixedName</code></td>
<td>Default name assigned to the element using this convention: devName-suffixMode-suffixType-suffixIndex1-suffixIndex2</td>
</tr>
<tr>
<td><code>vendor</code></td>
<td>Contents of vendor field. Usually, the vendor description string.</td>
</tr>
<tr>
<td><code>sysDescr</code></td>
<td>Contents of the sysDescr field.</td>
</tr>
<tr>
<td><code>sysLoc</code></td>
<td>Contents of the sysLocation field.</td>
</tr>
<tr>
<td><code>sysOid</code></td>
<td>Contents of the sysObjectID field.</td>
</tr>
<tr>
<td><code>sysName</code></td>
<td>Contents of the sysName field.</td>
</tr>
<tr>
<td><code>modifiedSysName</code></td>
<td>Contents of the sysName field with all quotation marks removed and the domain name truncated at the first period.</td>
</tr>
<tr>
<td><code>sysContact</code></td>
<td>Contents of the sysContact field.</td>
</tr>
<tr>
<td><code>ifDescr</code></td>
<td>Description of the element, usually contents of the ifDescr field.</td>
</tr>
<tr>
<td><code>ifType</code></td>
<td>Element type, usually contents of the ifType field.</td>
</tr>
<tr>
<td><code>pollAddr</code></td>
<td>Address to be polled, usually contents of the ifAddr field, but can be contents of the ifIpAddr if the DNS Lookup by ifIpAddress parameter is set to yes.</td>
</tr>
<tr>
<td><code>ifIpAddr</code></td>
<td>IP address associated with the interface being discovered.</td>
</tr>
</tbody>
</table>
The following table describes the eHealth functions you can use to customize element names.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| `snmpGet $Session oid var` | Sets `var` to the value retrieved from an SNMP get request on `oid`. The value for `var` must have the following form: 

```
{oid type value}
```

For example: `.1.3.6.1.2.1.1.5 DisplayString myNode` returns a value for status with 0 indicating success.

| `octetStringToAsciiText octetString` | Translates an octet string to ASCII text. Use this function for converting OctetStrings to DisplayStrings. |

The following example applies to LAN/WAN discoveries. It assumes that the `ifDescr` field is defined and unique for each MIB2 element in the network and is being used to set the element name:

```bash
1 #
2 # Custom Naming script sample for lanWan interfaces to be named after ifDescr
3 #
4 if {$Mode == "LanWanHealth"} {
5 #
6 # For lanWan discovery only
7 #
8 set IF_DESCR .1.3.6.1.2.1.2.2.1.2
9 catch {snmpGet $Session $IF_DESCR.$index descr} status
10 if {$status != 0} {
11 #
12 # No ifDescr available
13 #
14 return suffixedName
15 } else {
16 #
17 # Parse result and return ifDescr only
18 #
19 set ifDescrCooked [lindex $descr 2]
20 regsub -all " " $ifDescrCooked _ ifDescr
21 return "$sysName-$ifDescr"
22 } else {
23 #
24 # Naming schema not applicable
25 #
26 #
27 return suffixedName
28 }
```
Appendix C: Managing Alternate Latency

This appendix includes the following topics:

- Latency
- Alternate Latency Collection
- Alternate Latency Guidelines

Latency

eHealth obtains latency data about elements in the database by calculating round-trip latency, the time it takes for data to traverse your network from the sending system (eHealth system) to a receiving system (monitored element) and back. The round-trip time indicates the degree of activity in your network. However, eHealth can also collect alternate latency data from another source such as a Cisco router to a configured destination and back.

Alternate Latency Collection

Latency charts can indicate whether delays are caused by the network, an application, the user’s personal computer (PC), or the Internet connection. The alternate latency source is an element that can collect latency data from another device in your network, called the latency partner, as illustrated in this figure.
eHealth supports Cisco Systems, Inc. router agents with management information bases (MIBs) that support the Cisco Ping group as alternate latency sources. Typically, these MIBs are installed on Cisco devices that run IOS Release 10.2 or greater. If the Cisco router MIB supports the Cisco Ping group, you can use Cisco Ping as the latency data source instead of eHealth latency.

When eHealth polls the Cisco router, it asks the agent to start a ping process for each element that has a specified latency partner. For example, if you have one router parent element and 10 router interface elements, and all 11 elements have a latency partner, eHealth requests that the Cisco Agent start 11 ping processes. The Cisco router issues the ping requests and receives responses. Later, eHealth sends another SNMP request to the Cisco router to obtain the latency data. Thus, when you use alternate latency, you double the number of SNMP messages sent between eHealth and each latency source. The ping processes from each latency source also increase network traffic.

### How to Configure the Alternate Latency Ping Process

By default, at the alternate latency source, eHealth requests a ping test with default parameters for the ping packet size, number of ping packets, and the timeout rate. To modify these settings, you can define the environment variables described in the following table:

<table>
<thead>
<tr>
<th>Default Parameter Setting</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping packet sizes of 100 bytes</td>
<td>Define the NH_CISCO_PING_PKTSIZE environment variable and specify the size of the packet in bytes. If you do not define this variable, eHealth uses the value of NH_POLL_PING_PKTSIZE, which is 100 bytes by default.</td>
</tr>
<tr>
<td>5 ping packets</td>
<td>Define the NH_CISCO_PING_PKT_COUNT environment variable and specify the number of packets to send.</td>
</tr>
<tr>
<td>Timeout value of 2,000 milliseconds (2 seconds) for the ping request</td>
<td>Define the NH_CISCO_PING_TIMEOUT environment variable and specify the maximum number of milliseconds that the latency source should wait for a response to the ping request.</td>
</tr>
</tbody>
</table>

By default, eHealth bases ping latency calculations on a high-resolution Windows system clock. If you have systems with multiple CPUs, skewed data can result if each CPU bases its calculations on a different clock.

### Modify Alternate Latency Elements

When you discover LAN/WAN or router elements, eHealth automatically detects whether a discovered device supports alternate latency. To use alternate latency, you must specify a latency partner for the element. A latency source can have only one latency partner. If you want to measure latency from the same source to different partners, you must create a copy of the source element.
To examine the alternate latency configuration

1. In the Poller Configuration dialog, select the types of elements under List Elements of Type that you would like to display (such as LAN, WAN, or Router), and then click Latency.

   **Important!** The dialog lists only those elements currently shown in the Poller Configuration dialog that have Capable of Alternate Latency selected. The dialog is empty if the elements shown in the Poller Configuration dialog are not capable of alternate latency.

2. Examine the fields in the Latency column:
   - Device to Partner indicates that the element is collecting alternate latency.
   - Disabled indicates that it does not report latency information at all.
   - Poller to Device indicates that it collects eHealth latency.

3. Examine the Partner field, which shows the IP address of the configured latency partner. This field is empty if the element uses eHealth latency or if latency collection is disabled.

To modify elements that are capable of alternate latency, select an element in the Elements Capable of Alternate Latency dialog and click Modify. Specify the latency partner or change the latency collection settings as applicable. Make sure that the alternate latency source can ping the specified partner IP address.

**Alternate Latency Guidelines**

When you use alternate latency, follow these guidelines and practices:

- When you run Trend reports for latency, the element names include the IP addresses of latency partners. However, including the latency partner name in the element name can help you identify the element’s latency partner in reports. For example, if an element is named router-enet-port-1, and its latency partner is the device at 1.2.3.4, you could rename the element router-enet-port-1-to-1.2.3.4 or router-enet-port-1-to-NYRouter.

- If you change the element name, confirm that the name uses the supported element name characters. 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 (/). In Health reports, eHealth usually truncates the element name at 30 characters.

- Be sure to select Device to Partner to enable the collection of alternate latency information for this element and specify the IP address of the latency partner.

- To configure alternate latency, eHealth requires a read-write community string for the latency source. You might need to rediscover the source with a read-write string or modify the element to specify it.

- If you are modifying a router interface element to collect alternate latency data, select Record detail data to save the data for the interface.
Alternate Latency Guidelines

Create Multiple Latency Partners for an Element

You can specify only one latency partner for an alternate latency element. If you would like to generate Trend reports that show the latency from one interface element to multiple latency partners, you can create copies of the elements to specify a different latency partner. Each additional latency partner element that you create adds another element to the database disk space requirements and causes eHealth to poll the source device again.

To create an additional latency partner for an element

1. Click Latency in the Poller Configuration dialog and select an interface element. You cannot copy a router parent element to create additional latency sources.
2. Click Copy and specify the properties of the element. The default element name is copy-of-element. If this element exists in your database, you must specify a unique name. You might want to use a name that indicates the latency partner. For example, if the original element is named ChiRtr-enet-port-1, and the latency partner is the accounting server, you could name the element ChiRtr-enet-port-1-to-AcctServer. This element name also clarifies the latency partner in reports.

Delete Alternate Latency Elements

When you delete an element that supports alternate latency, you also delete any additional latency copies that you created for the element. For example, assume that you have a router interface element named CityRouter-enet-port-1, and you copied this element to make two additional latency partner elements: CityRouter-to-London and CityRouter-to-NYC. If you delete the original element, eHealth also deletes the copied elements. However, you can delete a copied element without deleting the original element.

Disable Alternate Latency Data Collection

If you are troubleshooting network utilization problems, you can disable alternate latency data collection for all elements that are configured to use Device-to-Partner alternate latency to stop that extra traffic. Set the NH_CISCO_PING_DISABLED environment variable to yes. If you change the variable value from yes to no, eHealth restores the latency data collection as specified in the configuration of each element.
Appendix D: Using Secondary Consoles

This appendix includes the following topics:
- Administration with Multiple Consoles
- Configure Secondary Consoles on UNIX Systems
- Configure Secondary Consoles on Windows Systems

Administration with Multiple Consoles

When multiple consoles are in use, the first administrator who attempts to perform a task obtains read-write access for that task. Subsequent admins who attempt to perform the same task (regardless of which console the administrator is using) is given read-only access or is prevented from accessing a dialog that is being used by another administrator.

You can allow administrators who might have responsibility for specific users (such as customers) to perform the following tasks for those users from secondary consoles:
- Edit or delete elements.
- Modify system scheduled jobs.
- Schedule, customize, and run reports.

However, secondary consoles consume system resources and can impact system performance. The primary eHealth console and any of the secondary consoles can run at local or remote workstations. Through the primary console, administrators can perform all administrative- and user-level eHealth tasks. Administrators can use secondary consoles to perform a subset of the tasks that can be performed from the primary console.

If you have several eHealth administrators at your site, each administrator can use an eHealth console to perform administrative tasks. The primary eHealth console and any of the secondary consoles can run at local or remote workstations. Through the primary console, administrators can perform all administrative- and user-level eHealth tasks. Administrators can use secondary consoles to perform a subset of the primary console tasks.
From the secondary console, an administrator can access some dialogs with restrictions. The following restrictions apply when an administrator opens the Poller Configuration dialog from the primary console or a secondary console:

- Poller Configuration dialog is accessible in read-only mode from the other console, unless you have filtered both consoles to show different groups.
- If you have specified different element filters for both consoles—from the console that you are using—you can access the Poller Configuration dialog in read-write mode for the group that is not appearing in the other console. It displays the elements for the group on which you are filtering only.
- If you have specified a filter on only one of the consoles or the same filter on both consoles, you can access the Poller Configuration dialog for the other in read-only mode only.

The following table explains how an open Poller Configuration dialog affects your ability to view or modify element information from the other dialogs on the primary and secondary consoles.

<table>
<thead>
<tr>
<th>Primary Console Filter</th>
<th>Primary Console Poller Configuration Dialog</th>
<th>Secondary Console Filter</th>
<th>Secondary Console Poller Configuration Dialog</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Inaccessible</td>
<td>N/A</td>
<td>Read-only</td>
</tr>
<tr>
<td>N/A</td>
<td>Read-only</td>
<td>N/A</td>
<td>Inaccessible</td>
</tr>
<tr>
<td>None</td>
<td>Open</td>
<td>None</td>
<td>Read-only</td>
</tr>
<tr>
<td>None</td>
<td>Read-only</td>
<td>None</td>
<td>Open</td>
</tr>
<tr>
<td>Grp A</td>
<td>Open</td>
<td>None</td>
<td>Read-only</td>
</tr>
<tr>
<td>Grp A</td>
<td>Open</td>
<td>Group A</td>
<td>Read-only</td>
</tr>
<tr>
<td>Grp A</td>
<td>Open</td>
<td>Group B</td>
<td>Read-write</td>
</tr>
<tr>
<td>Grp A</td>
<td>Read-write</td>
<td>Group B</td>
<td>Open</td>
</tr>
<tr>
<td>None</td>
<td>Read-only</td>
<td>Group B</td>
<td>Open</td>
</tr>
<tr>
<td>Grp B</td>
<td>Read-only</td>
<td>Group B</td>
<td>Open</td>
</tr>
</tbody>
</table>

eHealth displays messages to indicate whether you have read-only access, or to indicate that you cannot open a dialog. It also displays messages in each console about changes that all administrators are making.
Element Management

Only one eHealth administrator at a time can open the Poller Configuration dialog for editing, unless each console has specified the name of a group on which to filter. For both consoles to have read-write access, the group filters specified in the Set Element Filter field in the Options dialog must be unique.

- If element filters are not set, and a secondary administrator attempts to open the Poller Configuration dialog while an administrator is editing it, eHealth notifies the secondary administrator that the dialog can be opened in read-only mode only. The secondary administrator can then view it, but cannot modify it.

- If each console has a unique group specified in the Set Element Filter field, administrators can open their Poller Configuration dialogs to edit the elements in the groups they specified in the Set Element Filter field, even if other administrators are simultaneously modifying other groups of elements.

The first administrator to open the Poller Configuration dialog automatically receives read-write access. Other administrators who attempt to open the dialog while it is open are granted read-only access. Two administrators cannot work on the same group of elements or reports simultaneously. Administrators can, however, use element filters to display only the groups for which they are responsible in the Poller Configuration dialog, thus ensuring that they can modify the elements for which they are responsible while other administrators modify their own elements.

**Important!** Element filtering enables administrators to edit different groups at the same time. Because eHealth permits the same element to exist in more than one group, one administrator could overwrite changes made concurrently by another administrator. Therefore, take precautions to prevent two administrators from modifying the same elements at the same time.

Global Option Settings

You can set global console options to show alias names instead of element names and specify report time zones. When you change the settings for the time zone and alias name fields in a secondary eHealth console, the settings are not preserved for any subsequent console sessions. The global settings only apply to the console in which you apply them; that is, if you set an option in the primary console, it is not automatically enabled in the secondary console.

Job Scheduling

An eHealth administrator who uses a secondary console cannot modify scheduled system jobs. The primary eHealth administrator is responsible for managing the database and performing these functions. If two eHealth administrators modify the same scheduled job at the same time, eHealth saves only the changes that were saved last. It overwrites the changes that were saved first.
Configure Secondary Consoles on UNIX Systems

Before allowing other administrators to run eHealth at a secondary console, note the following restrictions. If you have installed eHealth on a UNIX system and you allow remote administrators access using secondary consoles, you must grant write permission to those other users. You must add the secondary console administrators to the UNIX user group to which the primary eHealth user account belongs.

Specify group write permissions for the following directories (and their subdirectories) in your eHealth installation:
- help
- log
- output
- poller
- reports
- tmp
- web/output
- eHealth/extensions/auto

To run a secondary console, each administrator must do the following
1. Log in as a different user (each eHealth administrator must use a unique user name).
2. Obtain read and write access permissions on eHealth directories to create, read, or modify a report or temporary file.

To register another administrator as a database user
1. Log in as the eHealth user (the name by which you or other administrators access eHealth) on the eHealth system.
2. Do one of the following:
   - If your shell is sh or ksh, source the nethealthrc.sh file.
   - If your shell is csh, source the nethealthrc.csh file.
3. Enter the following command to specify administrator privileges for the new user, where username is the name of an existing UNIX account:

   \texttt{nhManageUsers -add -user username -priv admin}

To run a secondary console at a remote UNIX workstation
1. Issue the following command, where \texttt{eHealthHost} is the name of the eHealth system:

   \texttt{xhost +eHealthHost}

   The X server can now access your display.
2. Log in to the eHealth system remotely by entering the following command:
   `rlogin eHealthHost`
   You are now logged in remotely.

3. Set the display to appear on your workstation by entering the following, where `systemName` is the name of the workstation on which you want to display the console:
   `setenv DISPLAY systemName:0.0`
   The console will now appear on the specified workstation.

4. Do one of the following:
   - If your shell is sh or ksh, source the `nethealthrc.sh` file.
   - If your shell is csh, source the `nethealthrc.csh` file.
   The file is sourced.

5. Enter the following command, where `eHealth` is the full pathname of the eHealth installation directory:
   `eHealth/bin/eHealth -2nd`
   The eHealth console appears.

### Configure Secondary Consoles on Windows Systems

You must create a new user to run the secondary console. (The same user cannot run both the primary and secondary consoles simultaneously.) If you want to restrict access to these users, you can use Windows access control lists to allow individual or group access.

**To register an administrator as a database user**

1. Log in as the eHealth user on the eHealth system.
   The login is successful.

2. Enter the following command to specify administrator privileges for the new user, where `username` is the user name of the secondary console administrator (the user name must be the name of an existing Windows user account):
   `nhManageUsers -add -user username -priv admin`
   The user can now perform administration tasks using the secondary console.

**Important!** If you run a secondary console on a Windows system, do not output on-demand or scheduled reports to the screen. If you have installed eHealth on a Windows system, you can obtain and install a Telnet server or Citrix Terminal Services on the eHealth system to support secondary consoles.
Use Terminal Services to Run a Secondary eHealth Console Remotely

Terminal servers are systems that run application server software that enables you to deploy and maintain a business-critical application on one server machine (or several servers), while multiple users access and use the application from end-user systems. If you plan to use Terminal Services, you must purchase and install the Exceed X server software. You cannot use XVision—the X server that is installed with eHealth—with Terminal Services.

To run a secondary console with Terminal Services

1. Confirm that Exceed and Terminal Services are installed on the terminal server on which eHealth resides.
2. Through the Control Panel, verify that the Administrative Tools directory includes shortcuts for the following:
   - Terminal Services Client Creator
   - Terminal Services Configuration
   - Terminal Services Licensing
   - Terminal Services Manager
3. Verify that Exceed appears in your list of programs.
4. Confirm that the Terminal Services client is running on the system that you are going to use as a secondary console.
5. Verify that XVision is not running on the Terminal Services server or client systems. If it is, stop the XVision Server. You cannot use it with Terminal Services.
6. Create user accounts for the system and for eHealth on the terminal server. Terminal Services supports a maximum of three users for secondary consoles.
7. Start the Exceed server on the terminal server.
8. Start the primary eHealth console, and then start the Terminal Services server.
9. Log in to the remote system (Terminal Services client) and start Exceed in the Terminal Services window.
10. Select Start, Run, enter cmd in the Open field, and click OK.
11. Enter the following at the command prompt, where x.x is the value that appeared in the Exceed window:

   set DISPLAY=:x.x

12. Start the secondary console on this system by entering the following command:

   eHealth -2nd
Use Telnet to Run a Secondary eHealth Console Remotely

If you are using a Telnet server and the client system (the system on which you want the secondary console to run) is running Windows, you must have an X server running. eHealth Windows installations provide XVision as the X server.

**To run a secondary console through telnet at a remote Windows workstation**

1. Confirm that the telnet server is installed.
2. Select Start, Programs, Vision, XVision Server, or start the primary eHealth console.
   The XVision server starts.
3. Log in to the eHealth system remotely by entering the following command:
   
   telnet eHealthHost
   The system logs you in.
4. Set the display to appear on your workstation by entering the following command, where *systemName* is the name of the workstation on which you want the console to appear:
   
   set DISPLAY=systemName:0.0
   The display is set.
5. Reset your TMPDIR environment variable by entering the following command, where *directoryName* is the name of the directory in which you want to create your tmp directory:
   
   set TMPDIR=directoryName/eHealth/tmp
   The environment variable is set.
6. Enter the following command:
   
   eHealth -2nd
   The secondary eHealth console is now available for use.
Appendix E: Customizing the eHealth Web User Interface and OneClickEH

This appendix includes the following topics:

- Customize the eHealth Web Site
- How to Create Report Shortcuts
- Advanced Customization of the Web User Interface
- Displaying Alias Names in eHealth
- Set the Date Format in eHealth
- Set the Time Format in eHealth
- Specify Date and Time Preferences for the OneClick for eHealth Interface
- Customize the User Administration Screen of the OneClick for eHealth Interface
- Customize OneClickEH Tables
- Save OneClickEH Table Entries

Customize the eHealth Web Site

When a user accesses the eHealth web server, the eHealth web site displays a standard welcome with a message of the day. Each web page appears with eHealth's template background. After the user logs in, the web navigation bar is displayed to allow users to access other eHealth web pages. The Site Configuration feature allows you to customize an eHealth site and the configuration of all web user accounts on that site in various ways, as outlined in the following table.

<table>
<thead>
<tr>
<th>Customization</th>
<th>Default Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace the welcome page background image file. You must specify an image file name in the Background image file field with a .gif extension and move the .gif file to the eHealth/web/output directory.</td>
<td>Blue, white, and green (eHealth does not specify a file name)</td>
</tr>
</tbody>
</table>
### Customize the eHealth Web Site

<table>
<thead>
<tr>
<th>Customization</th>
<th>Default Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the welcome page default text color by specifying a hexadecimal RGB</td>
<td>000000 (black)</td>
</tr>
<tr>
<td>value. For example, white is FFFFFF, and blue is 0000FF.</td>
<td></td>
</tr>
<tr>
<td>Change the maximum number of nodes that appear on the Run Traffic Accountant</td>
<td>500</td>
</tr>
<tr>
<td>Reports pages.</td>
<td></td>
</tr>
<tr>
<td>Change the maximum number of reports that appear on the Organization and</td>
<td>50</td>
</tr>
<tr>
<td>Report List pages. You can navigate to the next set of links using the list</td>
<td></td>
</tr>
<tr>
<td>page navigation links. If you specify a smaller number such as 25 or 50,</td>
<td></td>
</tr>
<tr>
<td>the list of reports appears very quickly. If you have a large number of</td>
<td></td>
</tr>
<tr>
<td>web reports (such as 200 or more) and you list them all on one page, the</td>
<td></td>
</tr>
<tr>
<td>list page will take longer to appear.</td>
<td></td>
</tr>
<tr>
<td>Change the maximum number of elements allowed in a range in the selection</td>
<td>500</td>
</tr>
<tr>
<td>lists included in Run Trend and At-a-Glance Report pages.</td>
<td></td>
</tr>
<tr>
<td>Modify the rate at which eHealth refreshes the Cluster Status.</td>
<td>5 minutes (or 300</td>
</tr>
<tr>
<td>seconds)</td>
<td></td>
</tr>
<tr>
<td>Change the amount of time that eHealth allows the Cluster Status utility</td>
<td>5 seconds</td>
</tr>
<tr>
<td>to attempt to determine the state of the cluster before timing out.</td>
<td></td>
</tr>
<tr>
<td>Enable Web security. By default, eHealth requires users to log in as web</td>
<td>Yes</td>
</tr>
<tr>
<td>users before they can view or run reports.</td>
<td></td>
</tr>
<tr>
<td><strong>Important!</strong> When you disable web security for a user, you disable the</td>
<td></td>
</tr>
<tr>
<td>user's access to all Live Health applications.</td>
<td></td>
</tr>
<tr>
<td>If you change this setting from No to Yes, eHealth automatically deletes</td>
<td></td>
</tr>
<tr>
<td>any existing MyHealth report pages for all web users at the eHealth site.</td>
<td></td>
</tr>
<tr>
<td>Correctly redirect the URL of their reports running through a proxy server.</td>
<td>No</td>
</tr>
<tr>
<td>By default, when the eHealth web server is running through a proxy server</td>
<td></td>
</tr>
<tr>
<td>with Internet Explorer, eHealth does not allow the server name to be passed</td>
<td></td>
</tr>
<tr>
<td>properly (for security reasons). As a result, any reports that a user</td>
<td></td>
</tr>
<tr>
<td>generates through this server will fail.</td>
<td></td>
</tr>
<tr>
<td>Hide the navigation bar and prevent users from accessing other eHealth web</td>
<td>Yes</td>
</tr>
<tr>
<td>interface pages. By default, eHealth shows the navigation bar to allow users</td>
<td></td>
</tr>
<tr>
<td>to access other web pages.</td>
<td></td>
</tr>
</tbody>
</table>
From the console, you can customize the eHealth Apache Web server to manage access to web reports and eHealth web pages.

**To customize your eHealth site**

1. Using a web browser, access the web server and log in as the admin user.
2. Select the Administration tab from the web navigation bar.
3. On the Administration page, select eHealth Management, and then select Site Configuration.
4. For any customization options, accept the default setting, enable or disable the setting, or specify a different value. Follow the guidelines provided in the table.
5. Click Save.

<table>
<thead>
<tr>
<th>Customization</th>
<th>Default Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent eHealth from performing a variable validation check for elements when the Web user sets up a Trend Report page.</td>
<td>Yes</td>
</tr>
<tr>
<td>Exclude from the selection lists any elements that are not being polled. By default, if eHealth does not poll an element, it still includes it in selection lists.</td>
<td>Yes</td>
</tr>
<tr>
<td>Show report templates on the Run Reports page for unlicensed element types. By default, if you do not have a license to poll an element type, eHealth does not display the report template for it on the Run Reports page.</td>
<td>No</td>
</tr>
<tr>
<td>Rotate the web server access log automatically to prevent it from becoming large enough to slow down the access log generation. By default, eHealth does not rotate the log file when it becomes too large.</td>
<td>No</td>
</tr>
<tr>
<td>Rotate the web server access log after the specified number of days. If you do not enable this option and specify a value, eHealth rotates the file after seven days by default.</td>
<td>7 days</td>
</tr>
<tr>
<td>Scan user input for potentially malicious HTML content.</td>
<td>No</td>
</tr>
<tr>
<td>Allow the use of Western European special characters (ISO8859-1) such as German accent/umlaut marks in element and group names.</td>
<td>Yes</td>
</tr>
<tr>
<td>Customize the message that appears on the Welcome page when web users log in. You can specify any text and include standard HTML tags to format your message.</td>
<td>Welcome to eHealth</td>
</tr>
</tbody>
</table>
How to Customize a Privacy Page for Your eHealth Site

Many organizations and legislative initiatives require that organizations place a publicly accessible document within their web applications that defines their information privacy policy. If you have a standard privacy document or plan to create one, you should make it accessible within your eHealth software installation.

To include a privacy policy web page within your eHealth software, do the following:
1. Create a web page that defines your policy.
2. Name the file privacy.html.
3. Save the file in the following directory:
   
   ```
   ehealth/web/output directory
   ```

How to Customize the Gateway Page for a Web User Account

A Gateway page can contain any kind of information or links that your users require concerning your products and services, as well the company itself. When you create or modify a web user account, you can set the Gateway page as the default initial page by changing the account permissions.

You can customize this page for an entire eHealth site or individual web user account. Within the Gateway page, you can include links to other pages, tools, web sites, or eHealth web interfaces. If you create a custom Gateway page for a web user account, the web interface uses that custom page only when that web user logs in to the web interface. For all other users, the interface displays the site Gateway page.

To create a custom Gateway page for a specific web user account, follow these steps:
1. Using any HTML editor, create a new gateway.html file in the `\eHealth\web\output\users\webUser` directory.
2. Save the customized Web page in the same directory. The `webUser` value represents the name of the web user account.
3. Although eHealth preserves the file during upgrades, it is good practice to create a backup copy and store it in another directory.

How to Customize the Gateway Page for the eHealth Site

You can customize the Gateway page for your site. However, if you have multiple Web user accounts and they require different information or access on their Gateway pages, you should create a custom Gateway page for each web user account.
To create a custom Gateway page for your eHealth site, follow these steps:

1. Using any HTML editor, create your new Gateway page, or edit the default Gateway page file in the \eHealth\web\output directory.
2. Save your custom web page in the \eHealth\web\output directory.

**Important!** Although eHealth preserves your custom gateway.html page during upgrades, it is good practice to create a backup copy and store it in another directory.

### How to Customize the eHealth Help

The online help files for the web interface and web-based reports consist of thousands of HTML files and GIF images saved in the \eHealth\web\help\files directory (and its subdirectories). In most cases, the link to the eHealth Help is a Help icon within the web interface page or the web report. You can modify the HTML help pages as well as add your own. However, if you change a help page that was installed with eHealth, eHealth overwrites the help page when you upgrade eHealth. If you create new files with names that eHealth does not use, it does not overwrite them during an upgrade.

The web pages use a Java script openHelpWin function to open the help page in a new web browser window. If you create a new web interface page that has help links, include the following Java script code to define this function.

```javascript
<script language='Javascript'> <!-- Hide script from old browsers
function openHelpWin( winName ) { msgWindow=window.open(winName,'_helpWin''toolbar=1,
location= 0,directories= 0,status= 0,menubar= 1, scrollbars= 1,resizable= 1,copyhistory=
1,width=600, height=500' ); msgWindow.focus();
} // finish hiding -->
</SCRIPT>
```

For examples, you can view the HTML page source or frame source for any web interface page that includes a Help icon or link.

### Customize Logo Images and Link Destinations

The navigation bar on each eHealth web page contains a company logo that links to the company web site. The logo is the logo2.gif file. The link, in the form of a URL, is contained in the logo2Link.txt file in the \eHealth\web\output directory.

You can customize pages for the site, as well as for individual web user accounts, by doing the following:

<table>
<thead>
<tr>
<th>Customization</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the GIF image for all web user accounts</td>
<td>Copy a new logo2.gif file to this directory and replace the text in the logo2Link.txt file.</td>
</tr>
<tr>
<td>Change the GIF image for the web user account userName directory.</td>
<td>Save your new GIF image and a copy of your modified logo2Link.txt file to the /eHealth/web/output/users/userName directory.</td>
</tr>
</tbody>
</table>
How to Create Report Shortcuts

How to Create Report Shortcuts

By default, eHealth allows web users to access At-a-Glance, Top N, and Trend report shortcuts on the Organization page (unless you modify the account setting to disable this feature for that user). You can also provide web users with additional shortcuts that allow them to run customized Trend and At-a-Glance reports for individual elements on demand from the Organization page, without having to use the Run Report user interface.

You can create a custom report template using the Save Report Template feature of the Run Reports page of the eHealth Web user interface and link to it within files provided in the /eHealth/web directory. You can create a customized shortcut for the following:

- All users at your eHealth site
- Individual web users

To meet the specific reporting needs of your eHealth site, you may need to create multiple customized report shortcuts to display on the Organization page.

---

Follow these guidelines when changing a logo or link on the eHealth web page:

- GIF images should be the same height as the default logo2.gif, which is 27 pixels.
- If a logo2.gif file appears in the userName directory, the web server uses your supplied logo2.gif image; otherwise, it uses the default eHealth image.
- If a logo3.gif file appears in either directory, the web server adds the logo to the web page.
- If you have a license for Live Health, you can customize the logo that appears in the upper-left corner of the Live Status diagram. For more information, see the eHealth Help.

---

<table>
<thead>
<tr>
<th>Customization</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a second logo in the upper right corner of each page for all web accounts.</td>
<td>Save the new GIF image as logo3.gif and replace the text in the logo3Link.txt file in the /eHealth/web/output directory.</td>
</tr>
<tr>
<td>Add a second logo for the web user account userName.</td>
<td>Save the new GIF image as logo3.gif and replace the text in the logo3Link.txt file in the /eHealth/web/output/users/userName directory.</td>
</tr>
</tbody>
</table>
Provide Report Shortcuts for an eHealth Site or Individual Users

To provide a customized At-a-Glance or Trend report shortcut on the Organization page of all web user accounts at your eHealth site, you can do one of the following:

- Create an XML file named toolbar.prop.usr which contains links to customized report templates, and place the file in the \eHealth\web\output directory.
- Make a copy of the toolbar.prop.usr.sample file provided in the \eHealth\web\output directory, rename it toolbar.prop.usr, and modify the file so that it links to your customized report templates.

If all Web users at your eHealth site do not need a specific report shortcut, you can create a single shortcut for the particular individual who needs it. When eHealth displays report shortcut icons on the Organization page, it uses any user-defined report shortcuts, if they exist. Otherwise, it uses shortcuts that have been defined for the entire site.

To create a customized report shortcut for your eHealth site or an individual web user

1. Log in to the eHealth web interface as the admin user, and then select the Run Reports tab.
2. On the Run Reports page, select Standard from the list of report templates under At-a-Glance or Trend in the Available Reports column. The specified Run Report page appears.
3. Create a template by supplying values for the appropriate fields.
4. Save the report settings as a customized report by specifying a name in the Template Name field. For example, if you chose Router/Switch as your technology, you could name it Router.
5. You can specify a maximum of 30 single-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). Space characters are not permitted.
6. Click Save Report Template. The following should occur:
   A template named Router should appear under Standard within the At-a-Glance or Trend report template list in the left pane of the Run Report page. eHealth generates a file named router.rpt and stores it in the /\eHealth\reports\glance\users\admin or /\eHealth\reports\trend\users\admin directory.
7. Do one of the following:
   - If you are creating a shortcut for an individual user, within the /\eHealth\web\output directory, locate the toolbar.prop.usr.sample file.
   - If you are creating a shortcut for an entire eHealth site, locate the toolbar.prop.usr file in the /\eHealth\web\output\users\webUserName directory.
8. Do one of the following:
   - Create another file named toolbar.prop.usr which contains references to customized report templates, as shown in this sample:

   **Note:** All tag names and properties values are case sensitive and should not contain any spaces and quotes.

   ```
   <Shortcuts>
   <Shortcut>
   <ReportType>(type trend or glance)</ReportType>
   <ReportTemplate>users/(account name)/Router</ReportTemplate>
   <ImageFile>/routerTrend.gif</ImageFile>
   </Shortcut>
   </Shortcuts>
   ```

   - Make a copy of the toolbar.prop.usr.sample file and rename it toolbar.prop.usr.

9. Open this toolbar.prop.usr file and complete the following:
   - For Trend report shortcut, specify `trend` for the ReportType tag. For example:
     ```
     <ReportType>trend</ReportType>
     ```
   - For At-A-Glance report shortcut, specify `glance` for the ReportType tag. For example:
     ```
     <ReportType>glance</ReportType>
     ```
   - Provide the path to the report template created in Step 6. For example:
     ```
     <ReportTemplate>users/admin/Router</ReportTemplate>
     ```
   - Provide the GIF image file that appears on the shortcut icon. For example:
     ```
     <ImageFile>/routerTrend.gif</ImageFile>
     ```

   **Important!** The new GIF file should be approximately 35 x 35 pixels.

10. Place a copy of the image file in the `/eHealth/web/output` directory.
    
    If the web user has enabled the Run an AAG Report shortcut or the Run a Trend Report shortcut using the User Preferences option under User Management on the Administration page, the appropriate icon will appear at the top of the Organization page. If you do not customize the image for the customized report icon, eHealth will use the same graphic for both icons.


12. Select the Organization tab at the top of the web interface page. The Organization page appears.

13. Click the plus sign (+) next to Elements in the left pane, and then select an element.

14. Click the shortcut icon. eHealth generates an At-a-Glance or Trend report for that element using the specified Router report template and displays it.

15. (Optional) Create additional shortcuts for your eHealth site:
   
   a. Create customized report templates using the Save Report Template feature of the Run Reports page of the eHealth web user interface.
b. Add the appropriate link to the toolbar.prop.usr file. For example:

```
<Shortcuts>
  <Shortcut>
    <ReportType>trend</ReportType>
    <ReportTemplate>user/admin/Router</ReportTemplate>
    <ImageFile>/routerTrend.gif</ImageFile>
  </Shortcut>
  <Shortcut>
    <ReportType>trend</ReportType>
    <ReportTemplate>user/admin/LanWan</ReportTemplate>
    <ImageFile>/lanwanTrend.gif</ImageFile>
  </Shortcut>
  <Shortcut>
    <ReportType>glance</ReportType>
    <ReportTemplate>user/ehealth/System</ReportTemplate>
    <ImageFile>/systemAAG.gif</ImageFile>
  </Shortcut>
</Shortcuts>
```

**Important!** The report shortcut will not use the appropriate report template unless the template .rpt file name matches the reference that appears in the toolbar.prop.usr file for that shortcut.

---

**Advanced Customization of the Web User Interface**

The web interface files reside on the eHealth system in the `/eHealth/web` directory. You can customize the web interface in the following ways:

- Create links to eHealth applications and links to pages and reports.
- Customize the user privileges configuration that the eHealth Apache web server uses to manage access to web reports and eHealth web pages.

**Creating Customized Links**

By customizing the web user interface files, you can create links that display web interface pages with preselected defaults, launch eHealth applications, automatically generate reports.
Creating Links to eHealth Applications

You can create links to open eHealth application windows from a page other than the Live Health page. Live Trend is an application that creates a chart to show the value of one or more variables for one or more elements. You select the elements and the variables that you want to display, and the Live Trend chart shows the data retrieved each time that eHealth polls the elements. You can create a link to open the Live Trend application window from a page other than the Live Health page. For example, you could add the following HTML code to a page such as the gateway.html page:

```
<SCRIPT LANGUAGE=JavaScript>
function openLiveTrendWin() { ltWindow = window.open ("/cgi-bin/nhWeb?func=livetrend","_blank","toolbar=0,location=0,directories=0,status=0,
menubar=0,scrollbars=0,resizable=0,width=500,height=40"); ltWindow.focus ();
</SCRIPT><A HREF="javascript:openLiveTrendWin()">LT</A>
```

You could also create an HREF link to nhWeb as follows:

```
<A HREF="http://webServerUrl/cgi-bin/nhWeb?func=livetrend" TARGET="_blank">Run the LiveTrend Application</A>
```

Live Exceptions is an application that shows the outstanding alarms for elements. You can create a link to open the Live Exceptions browser from a page other than the Live Health page. For example, you could add the following HTML code to a page such as the gateway.html page:

```
<SCRIPT LANGUAGE="JavaScript"> <!--
function leBrowserOpen()
{window.open("/cgi-bin/nhWeb?func=liveexceptions","_blank",
"toolbar=0,location=0,directories=0,status=0,menubar=0,scrollbars=1,
resizable=1,width=500,height=250")}
//--></SCRIPT>
<a href="javascript:leBrowserOpen()">Launch Live Exceptions</a>
```

You could also create an HREF link to nhWeb as follows:

```
<A HREF="http://webServerUrl/cgi-bin/nhWeb?func=liveexceptions" TARGET="_blank">Launch Live Exceptions</A>
```

For a complete description, see the eHealth Help for the specific application.

Create Links to Pages and Reports

eHealth uses the nhWeb common gateway interface (CGI) program and Java Servlets to produce the tabbed pages and report functions within the web interface.

The nhWeb CGI program is stored in the eHealth/web/cgi-bin directory. Depending on the options that you specify for nhWeb, you can create links to the following:

- Report List page with preselected report list filter values
- Organization page with expanded lists in the Organization tree
- Other tabbed pages in the web interface (such as the Gateway page or Administration page)
**Note:** When using nhWeb in HTML HREFs or http:// links, do not include space characters, carriage returns, or new lines within the URL. Also, replace any required spaces in variable names or other values with the plus (+) character or %20.

You can also customize a user's report generation in the following ways:

- Create links to the Run Reports page with preselected report criteria.
- Automatically bypass the Run Reports page and generate specific reports.
- Provide shortcuts on the Organization page to customized report templates.

If you log in to the OneClick for eHealth console as the web administrator, you can control the types of reports that your web users generate by specifying the contents of the Run Reports page for that user (providing access to run only certain types of reports, as well as certain named report definitions). If you have the eHealth Developer Program license, you can create or customize reports to add drilldown links to reports or other pages.

The Traffic Accountant reports that are available from the web interface do not use the nhWeb program; therefore, you cannot link to these reports or create URLs to run them.

### Link to the Report List Page

You can create links to the Organization and Report List pages and preselect the report list filter values. These links allow you to customize and control the default report list for your web users. However, regardless of the report filter settings, the filters show only those reports for the groups, group lists, and elements that the web user account is permitted to view.

### Format of Report List URL

The URL of a report list has the following format:

```
http://webServerUrl/cgi-bin/nhWeb?func=tabName&filterName=value&hideFilters=boolean
```

The format uses the following arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webServerUrl</code></td>
<td>The URL that you specify to access the eHealth web server. You should include <a href="http://webServerUrl">http://webServerUrl</a> only for links to pages on a remote eHealth web server.</td>
</tr>
<tr>
<td><code>tabName</code></td>
<td>Name of the tabbed page to display. You can specify either orgFrame (Organization page) or listFrame (Report List page) to link to the pages that use report lists.</td>
</tr>
</tbody>
</table>
This table lists the report filter settings:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filterName=value</code></td>
<td>Name of the filter that you want to set and its value. You can specify only one value for each filter argument. You can specify several filter options by separating each <code>filterName=value</code> string with an ampersand (&amp;). The report list shows only those reports that match all filter criteria. If you do not specify a filter and its value, the link uses the default value for that filter. The following table lists the filter names, descriptions, and values.</td>
</tr>
<tr>
<td><code>hideFilters=boolean</code></td>
<td>Specifies whether you want to hide the report list filter options. If you specify yes, the page does not show the report list filters; instead, it displays a link to display the filters. You can replace the link with arrow selections. If you specify no, the page shows the report list filters, which allow the web user to change the filter criteria and display other reports. The default is no.</td>
</tr>
</tbody>
</table>

This table lists the report filter settings:

<table>
<thead>
<tr>
<th><code>filterName</code></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fltrDate=value</code></td>
<td>Shows only the reports that were created for a specific time period. The valid values are today, prevHour, prev4hours, prev12hours, yesterday, thisWeek, lastWeek, thisMonth, lastMonth, and every. The default is every.</td>
</tr>
<tr>
<td><code>fltrJobId=value</code></td>
<td>Shows the history list for the specified job identification (ID). Specify the job ID value for the scheduled report as seen in the Schedule Jobs dialog. The default is 0 to show all scheduled reports.</td>
</tr>
<tr>
<td><code>fltrRptOrigin=value</code></td>
<td>Shows only the reports created by the specified method. eHealth administrators can schedule reports to run automatically as well as run reports on demand from the eHealth console. Web users can run reports on demand from the web interface. The valid values are all (to show both scheduled and on-demand reports), scheduledOnly, and nonScheduledOnly (to show on-demand reports only). The default is all.</td>
</tr>
<tr>
<td><code>fltrRptType=value</code></td>
<td>Shows only the reports of the specified report type. The valid values are glance, trend, traffic, topN, service, health, and every. The default is every.</td>
</tr>
</tbody>
</table>
Report List Example

The following URL displays the Report List page on the eHealth web server ne-sales and sets the report filter to show WAN reports. Since the URL does not specify the other filter criteria, it uses the default filter values. The report list shows all reports (of any type) for all WAN elements, and groups and group lists of WAN elements. The other filters use the default values.

http://ne-sales/cgi-bin/nhWeb?func=listFrame&fltrTech=wan

You can code this link in an HTML A HREF tag in a web page, as follows:

```html
<A HREF="http://ne-sales/cgi-bin/nhWeb?func=listFrame&fltrTech=wan" TARGET="_top">Go to Report List Page</A>
```

When a user clicks the link, the web server performs a security check.

Link to an Expanded Organization Page

You can use nhWeb to display the Organization page and specify additional arguments to expand the lists in the organization tree (the bottom left frame of the Organization page). The nhWeb URL to the Organization page has the following format:

http://webServerUrl/cgi-bin/nhWeb?func=orgFrame&expl=topLevel&explGrp=topLevel:subLevel& filterName=value&hideFilters=boolean
The orgFrame URL uses the same arguments that you use to customize a report list, as well as the following additional arguments:

- `expl=topLevel` expands the contents of a top-level organization type. For the top-level types, you can specify the name of a group list or AllGroupLists; a Traffic Accountant view; or the value AllGroups (all statistics groups), AllGroupLists (all statistics group lists), AllElems (all elements), or AllNodes (Traffic Accountant nodes).
- `explGrp=topLevel:subLevel` expands the contents of a sublevel below a specific top level. For the sublevel types, you can specify the name of a group within a group list or Traffic Accountant view, or an element range within a group.
- `pageTarget=anchorname` scrolls the left-hand frame to the specified anchor.

To target a group list in the GroupList section, use the following format:

```
gl_grouplistname
```

To target a group exploded in a group list, use the following format:

```
gl_grouplistname_groupname
```

To target an element inside a group inside an exploded group list, use the following format:

```
gl_grouplistname_groupname_elementname
```

To target a group (in the Groups section), use the following format:

```
grp_groupname
```

To target an element inside a group (in the Group section), use the following format:

```
grp_groupname_elementname
```

To expand several areas of the organization tree, you can specify a colon-separated string of expansion arguments. For example, the following string expands:

```
allGroupLists:groupList:group:toplevel:sublevel:subsublevel
```

**Organization Page Example**

The following URL displays the Organization page on the eHealth Web server seattle, expands the PostSales group list and the Corporate Traffic Accountant view, and expands the East group within the PostSales group list. The filter criteria causes the report list to show all Health reports (scheduled or on-demand) for the East group. The page hides the Report List page filter options.

```
http://seattle/cgi-bin/nhWeb?func=orgFrame&expl=AllGroupLists,
Corporate TAV&explGrp=AllGroupLists: East&fltRptOrigin=All&fltRptType=
health&fltRptSubject=East&hideFilters=yes
```
You can code this URL in an HTML HREF tag in a web page, as follows:

```
<A HREF="http://seattle/cgi-bin/nhWeb?func=orgFrame&expl=PostSales&expGrp=PostSales:East,Corporate_TAV&fltrRptOrig=All&fltrRptType=health&hideFilters=yes" TARGET="_top">Go to ReportList Page</A>
```

When a user clicks the link, the web server performs a security check.

**Link to Tabbed Pages**

To display a tabbed page in the web interface, use the following format of the `nhWeb` program:

```
http://webServerUrl/cgi-bin/nhWeb?func=tabName
```

You should omit `http://webServerUrl` for links that you specify in pages that are local to the web server; that is, pages that reside in the `eHealth/web/output` directory. If your web server domain name changes for any reason, you will not have to change your custom links. The link uses the following arguments:

- `webServerUrl` is the URL for the hostname/domain or IP address of your web server.
  - **Important!** You should include `http://webServerUrl` only for links to pages on a remote eHealth web server.
- `tabName` is the name of the tabbed page to display:
  - mainChoice (main choice page; this is the initial page defined for the web user account that logs in)
  - gatewayFrame (Gateway page)
  - orgFrame (Organization page)
  - listFrame (Report List page)
  - runFrame (Run Reports page)
  - myHealthFrame (MyHealth page)
  - toolsFrame (Live Health page)
  - aviewFrame (Systems & Apps page)
  - adminFrame (Administration page)
  - reportsFrame (Report Center page)

If you use `nhWeb` to link to the Organization page, Run Reports page, and Report List page, you can specify additional arguments that provide more customization capabilities.
Page Link Example

The following nhWeb example displays the Administration page on the eHealth web server miami.

http://miami/cgi-bin/nhWeb?func=adminFrame

You could type the preceding example as the URL address in a web browser; however, you would typically create a link to the URL using the HTML HREF tag in a web page, as shown in the following example.

<A HREF="http://miami/cgi-bin/nhWeb?func=adminFrame">Go to Administration page</A>

Link Security Actions

When a user clicks an eHealth link, the following security check is performed:

- If the web server uses authenticated access, it displays the login prompt for a web user name and password the first time that the user accesses the site. The user must specify a valid web user name and password (and must have the correct user account permissions) to access the page. Any subsequent links to that web site using the same web browser session will bypass the login.
- If the web server uses unauthenticated access, it displays the page without displaying a login prompt. In all cases, if the web user does not have permission to view the page, the web server displays a message to inform the user.
- If the page that has the link to nhWeb is part of a frameset, include the TARGET="_top" HTML code as follows:

  <A HREF="http://miami/cgi-bin/nhWeb?func=adminFrame" TARGET="_top">Go to Administration Page</A>

The TARGET="_top" code causes the web browser to replace the entire browser window with the new page. Otherwise, the web browser replaces only the frame in which the link appeared.

Link to a Run Reports Page

To display a Run Reports page with preselected report criteria, you specify the nhWeb program with the following format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&...

The arguments vary for each type of report that you can run, and not all arguments are required. You can specify the arguments in any order:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline=baseline</td>
<td>For a Situations to Watch Detail report, specifies the number of days or weeks in the baseline.</td>
</tr>
<tr>
<td>baselineType=type</td>
<td>For a Situations to Watch Detail report, specifies whether the baseline is in days or weeks. The default is days.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chartType=chart</td>
<td>For a Trend report, specifies the format of the chart. The valid values are lineStandard, line100, pie, barStandard, barStacked, bar100, and table. The default is lineStandard.</td>
</tr>
<tr>
<td>dayOptions=day</td>
<td>Specifies the days to include in the report for time ranges that span more than one day. The valid values are sun, mon, tue, wed, thu, fri, and sat. By default, eHealth includes all days. You can specify a comma-separated list of days. For example: dayOptions=mon,tue,wed (you cannot use spaces)</td>
</tr>
<tr>
<td>divBy=divide</td>
<td>For a Trend report, specifies that the chart display the variable value divided by a specified value. The valid values are none, time, frames, errors, and cells (for ATM elements). The default is time.</td>
</tr>
<tr>
<td>enableScalingPercentAxis</td>
<td>Specifies whether eHealth should use user-scaled axis values in the Trend and What-If Capacity Trend report graphs rather than auto-scaled values. The valid values are yes and no.</td>
</tr>
<tr>
<td>execute=Generate+Report</td>
<td>If you specify func=run, you must specify execute=Generate+Report to run the report automatically.</td>
</tr>
<tr>
<td>fromDate=startDate</td>
<td>If you specify timeRangeType=custom, specifies the starting date for the report time range. The valid value is a date in mm/dd/yyyy format.</td>
</tr>
<tr>
<td>fromTime=startTime</td>
<td>If you specify timeRangeType=custom, specifies the starting time for the report time range. The valid value is a time in hh:mm format with an AM or PM designation such as 09:30+AM. You cannot specify the fromTime argument for Service Level reports, Health reports, or Situations to Watch Detail reports.</td>
</tr>
<tr>
<td>func=function</td>
<td>Specifies the nhWeb command action. Specify one of the following: run to run a report; liveTrend to run the Live Trend application; liveExceptions to run the Live Exceptions application; or runFrame to display the Run Report page for that report type.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>goal1=goal</td>
<td>Specifies the goal value for each topNvarN variable that you specify. Specify goal1 for topNvar1, goal2 for topNvar2, and so on. The Top N report shows the difference between the actual value and the goal.</td>
</tr>
<tr>
<td>goal2=goal</td>
<td></td>
</tr>
<tr>
<td>goal3=goal</td>
<td></td>
</tr>
<tr>
<td>goal4=goal</td>
<td></td>
</tr>
<tr>
<td>goal5=goal</td>
<td></td>
</tr>
<tr>
<td>goal6=goal</td>
<td></td>
</tr>
<tr>
<td>goalLineLabel=label</td>
<td>Specifies the string that appears next to the goal line marker in the What-If Capacity Trend report graph.</td>
</tr>
<tr>
<td>goalLineValue=value</td>
<td>Specifies the value of the goal marker line that eHealth uses in the What-If Capacity Trend report graph.</td>
</tr>
<tr>
<td>granularity=sample</td>
<td>For a Trend, Service Level, or At-a-Glance report, specifies the sample size of the data. For Trend and At-a-Glance reports, the available values are 5-Minute Samples, 15-Minute Samples, Hour Samples, Day Samples, Week Samples, Month Samples, Quarter Samples, and Total. The default is asIs. For Service Level reports, the available values are Day, Week, and Month. The default is Day.</td>
</tr>
<tr>
<td>localized=value</td>
<td>Specifies whether the date and time values specified in any Date or Time arguments are localized. The valid values are yes and no. The default is no, which assumes that the date is in mm/dd/yyyy format. If you specify no, the nhWeb program converts the specified date and time values into the format that the eHealth system on the specified webServerUrl is configured to use. If you specify yes, the nhWeb program passes the date and time values directly to the Web server as specified. If the date and time formats do not match the formats required by the Web server, the Run Reports page might not load correctly.</td>
</tr>
<tr>
<td>maxYValuePercentAxis=value</td>
<td>Specifies the maximum value to which eHealth should set the vertical axis (y axis) when displaying percentage values.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mediumType=medium</td>
<td>Specifies the technology type of the subject. The valid values for this argument depend on the subjectType of report that you run. If you specify subjectType=group, the valid values are lan, wan, router, system, ras, qos, modemPool, modems, respPath, and respEndpoint. The default is the first type (in the order specified) that you support, which is usually lan. If you specify subjectType=grouplist, the valid values are lan, wan, lanWan, router, system, ras, qos, modemPool, modems, respPath, respEndpoint, and multiTechnology. The default is the first type (in the order specified) that you support, which is usually lan. If you specify subjectType=element, the following values are valid: adaptiveRateDsl, alcatelDevice, alcatelSlot, altBaseElement, apacheAppSvc, apacheAppSvcProcessSet, appRespPath, appService, appSvcProcessSet, applicationService, applicationServiceProcessSet, atmChannel, atmPvc, atmWanChannelSide, atmWanChannelSideCXR, atmWanChannelSidePeak, atmWanIf, atmWanPathSide, atmWanPathSideCXR, atmWanPort, atmWanPortPeak, backplane, bgProcessSet, bmcDisk, bmcNtSysPartition, bmcNtSystem, bmcNtUserPartition, bmcUnixSysPartition, bmcUnixSystem, bmcUnixUserPartition, cableLan, cableLanDownStreamChnl, cableLanUpStreamChnl, cacheAppliance, ccmConfMgrAppSvc, ccmCtiMgrAppSvc, ccmMsgIntAppSvc, ccmWebAttAppSvc, circuit, ciscoPopChannel, ciscoRasChannelizedT1E1, ciscoRemoteAccess, ciscoVPN3000, commWorksHA, commWorksHACN, commWorksHASTats, commWorksIWF, commWorksIWFCCS, commWorksIWFMS, commWorksIWFModemsAD, commWorksIWFModemsFAX, commWorksIWFPBS, commWorksIWFPPP, commWorksIWFQNC, commWorksIWFDTM, commWorksPDSN, commWorksPDSNAAA,</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mediumType=medium</td>
<td>If you specify subjectType=element, the following values are valid:</td>
</tr>
<tr>
<td>(continued)</td>
<td>comWorksPDSNFA1, comWorksPDSNFA2, comWorksPDSNIP, comWorksPDSNPPP,</td>
</tr>
<tr>
<td></td>
<td>comWorksPDSNVHA, component, cpu device, deviceEventSource, dialogProbe,</td>
</tr>
<tr>
<td></td>
<td>disk, diskPartition, dnsAppSvc,</td>
</tr>
<tr>
<td></td>
<td>dnsAppSvcProcessSet, ds1If, ds3If,</td>
</tr>
<tr>
<td></td>
<td>dslWanIf, dspCard, eHealthAppSvc,</td>
</tr>
<tr>
<td></td>
<td>eHealthAppSvcProcessSet, endToEnd,</td>
</tr>
<tr>
<td></td>
<td>envCpu, ethernetIf, ethernetSegmentIf,</td>
</tr>
<tr>
<td></td>
<td>eventSource, exchangeAppSvc,</td>
</tr>
<tr>
<td></td>
<td>exchangeAppSvcProcessSet,</td>
</tr>
<tr>
<td></td>
<td>excludedNtProcessSet, excludedProcessSet,</td>
</tr>
<tr>
<td></td>
<td>excludedUnixProcessSet,</td>
</tr>
<tr>
<td></td>
<td>fibreChannelIf, fixedRateDsl, frameRelayCircuit,</td>
</tr>
<tr>
<td></td>
<td>frameRelayPvcSidePeak, frameRelayWanIf,</td>
</tr>
<tr>
<td></td>
<td>fsRespPath, fw1EnforcementPtAppSvc,</td>
</tr>
<tr>
<td></td>
<td>fw1EnforcementPtAppSvcProcessSet,</td>
</tr>
<tr>
<td></td>
<td>fw1MgmtStationAppSvc,</td>
</tr>
<tr>
<td></td>
<td>fw1MgmtStationAppSvcProcessSet,</td>
</tr>
<tr>
<td></td>
<td>FrameRelayPvc, frameRelagenericAppSvc,</td>
</tr>
<tr>
<td></td>
<td>genericAppSvcProcessSet, genericAtmChannel,</td>
</tr>
<tr>
<td></td>
<td>genericCCMAppSvc, yPvcSide, genericCallMng,</td>
</tr>
<tr>
<td></td>
<td>genericDisk, genericDspCard, genericEventSource,</td>
</tr>
<tr>
<td></td>
<td>genericLanIf, genericModem,</td>
</tr>
<tr>
<td></td>
<td>genericModemPool, genericRas,</td>
</tr>
<tr>
<td></td>
<td>genericRespClientSet, genericRespDst,</td>
</tr>
<tr>
<td></td>
<td>genericRespPath, genericRespPathSet,</td>
</tr>
<tr>
<td></td>
<td>genericRespSrc, genericRouterSwitch,</td>
</tr>
<tr>
<td></td>
<td>genericRouterSwitchCpu, genericSysPartition,</td>
</tr>
<tr>
<td></td>
<td>genericSystem, genericUserPartition,</td>
</tr>
<tr>
<td></td>
<td>genericWanIf, genericWanIfPeak, GTPTunnel,</td>
</tr>
<tr>
<td></td>
<td>httpProxy, iisAppSvc, iisAppSvcProcessSet,</td>
</tr>
<tr>
<td></td>
<td>ikeTunnel, insightSystem, interface,</td>
</tr>
<tr>
<td></td>
<td>internetAppliance, ipsecTunnel, isdnModem,</td>
</tr>
<tr>
<td></td>
<td>justDiscovered, lan, lanIf, lanWan,</td>
</tr>
<tr>
<td></td>
<td>lotusNotesAppSvc,</td>
</tr>
<tr>
<td></td>
<td>lotusNotesAppSvcProcessSet, lucentPCF,</td>
</tr>
<tr>
<td></td>
<td>lucentPCFFRBC, lucentPCFRAS,</td>
</tr>
<tr>
<td></td>
<td>manageWiseSystem, mdbSwanIf,</td>
</tr>
<tr>
<td></td>
<td>mobilewirelessIf, mobilewirelessModemIf,</td>
</tr>
<tr>
<td></td>
<td>mobilewirelessRasIf, mobilewirelessRouterIf,</td>
</tr>
<tr>
<td></td>
<td>modem, modemPool, modems,</td>
</tr>
<tr>
<td></td>
<td>msSqlServerAppSvc,</td>
</tr>
<tr>
<td></td>
<td>msSqlServerAppSvcProcessSet, multiTech,</td>
</tr>
<tr>
<td></td>
<td>multiTechnology, narrowBandTrunk,</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mediumType=medium (continued)</td>
<td>If you specify subjectType=element, the following values are valid: (continued)</td>
</tr>
</tbody>
</table>
mediumType=medium
(continued)

If you specify subjectType=element, the following values are valid: (continued)

- sysEdgeEventSource, sysEdgeNtSysPartition, sysEdgeNtSystem, sysEdgeNtUserPartition, sysEdgeRespPath, sysEdgeUnixSysPartition, sysEdgeUnixSystem, sysEdgeUnixUserPartition, sysPartition, system, systemCpu, systemPartition, tokenRingIf, trakkerProbe, unixProcess, unixProcessSet, unknown, unlicensedSysEdge, userApp1AppSvc, userPartition, utilityElement, virtualSession, visualFrameRelayPvcSide, voiceDs0, voiceGateway, voiceGatewayCpu, voicePeerToPeerLink, vpnIf wan, wanIf, webAppSvc, webAppSvcProcessSet, winphoriaActiveDirectory, winphoriaCPU, winphoriaControlSwitch, wirelessLan, as well as any custom element types that you create. The default is the first type (in the order specified) that you support, which is usually ethernetIf.

If the value has spaces, replace each space with a plus (+) or %20 when you specify it in the nhWeb program.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nameFilter=filter</td>
<td>Specifies the subject list filter for the Run Reports page. The valid value is a string such as Blue* to list only the subject names that begin with the string Blue. You can specify expressions such as <em>blue, blue</em>, or <em>blue</em> to list elements that match the search criteria. Specify * to display all subject names that match the other subject criteria. You can specify up to 80 characters for the string.</td>
</tr>
<tr>
<td>partialDayStart=time</td>
<td>If you specify timeOptions=includeHrs, specifies the start time for reports that include only specific hours within the time range. The valid value is in the format hh+AM or hh+PM.</td>
</tr>
<tr>
<td>partialDayStop=time</td>
<td>If you specify timeOptions=includeHrs, specifies the end time for reports that include only specific hours within the time range. The valid value is in the format hh+AM or hh+PM.</td>
</tr>
</tbody>
</table>
For drilldown reports such as Health Index Detail, Trend, and At-a-Glance reports that can include specific days, specifies the days to include in the report. The valid value is a string in the format SMTWTFS where each letter represents a day in the week in order from Sunday through Saturday. Specify the letter of the day to include or a dash (-) otherwise. For example, to include all days except Friday and Saturday, specify SMTWT-. You cannot use partialWeek in place of dayOptions for a Run Report page link.

For Response Health and Service Level reports, specifies the protocol to include in the report. You can specify a comma-separated list of protocols as follows:

```
protocol=protocola,protocolb
```

You cannot specify space characters in the value string. To obtain the list of allowable protocol values, use the Run Health Report or Run Service Level Report page. Select the correct technology in the Technology list. After the page refreshes, right-click in the Run Health Report or Run Service Level Report page and select View Frame Source. The HTML source lists all valid protocol values. Use the protocol string specified for each OPTION VALUE=string under the NAME=protocol code.

For Response Service Level reports, specifies the protocol to include in the report. You can specify a comma-separated list of protocols as follows:

```
protocol=protocol2
```

You cannot specify space characters in the value string. To obtain the list of allowable protocol2 values, use the Run Service Level Report page. Select the correct technology from the Technology list. After the page refreshes, right-click in the Run Service Level Report page and select View Frame Source. The HTML source lists all valid protocol2 values. Use the protocol2 string specified for each OPTION VALUE=string under the NAME=protocol2 code.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>partialWeek</td>
<td>For drilldown reports such as Health Index Detail, Trend, and At-a-Glance reports that can include specific days, specifies the days to include in the report. The valid value is a string in the format SMTWTFS where each letter represents a day in the week in order from Sunday through Saturday. Specify the letter of the day to include or a dash (-) otherwise. For example, to include all days except Friday and Saturday, specify SMTWT-. You cannot use partialWeek in place of dayOptions for a Run Report page link.</td>
</tr>
<tr>
<td>protocol</td>
<td>For Response Health and Service Level reports, specifies the protocol to include in the report. You can specify a comma-separated list of protocols as follows: protocol=protocola,protocolb  You cannot specify space characters in the value string. To obtain the list of allowable protocol values, use the Run Health Report or Run Service Level Report page. Select the correct technology in the Technology list. After the page refreshes, right-click in the Run Health Report or Run Service Level Report page and select View Frame Source. The HTML source lists all valid protocol values. Use the protocol string specified for each OPTION VALUE=string under the NAME=protocol code.</td>
</tr>
<tr>
<td>protocol2</td>
<td>For Response Service Level reports, specifies the protocol to include in the report. You can specify a comma-separated list of protocols as follows: protocol=protocol2,protocol2  You cannot specify space characters in the value string. To obtain the list of allowable protocol2 values, use the Run Service Level Report page. Select the correct technology from the Technology list. After the page refreshes, right-click in the Run Service Level Report page and select View Frame Source. The HTML source lists all valid protocol2 values. Use the protocol2 string specified for each OPTION VALUE=string under the NAME=protocol2 code.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report=reportName</td>
<td>Specifies the name of the report to run. eHealth provides some default report names such as Standard, but eHealth administrators and Developer Program users can create additional, custom reports. Specify the name of a report as shown in the Run Report dialog boxes on the eHealth console, or as the links that appear below each report type on the Run Reports page. Do not include the .rpt suffix that appears on the report file name. The names of the drilldown only reports include TopTenComponents, AllComponents, HealthIndexDetail, and SituationsTrend.</td>
</tr>
<tr>
<td>reportType=type</td>
<td>Specifies the type of report to run. The valid values are health, service (or service+level), glance (or at+a+glance), trend, topn, whatIf, and drilldown. (You cannot use nhWeb to run Traffic Accountant reports.) The drilldown reports include special reports that are only available as drilldowns from the eHealth Web user interface. These reports include the Health Index Detail report, the Situations to Watch Detail report, the Top Ten Components report, and the All Components report.</td>
</tr>
<tr>
<td>serviceProfile=profile</td>
<td>For a Health Index Detail report or Situations to Watch Detail report, specifies the name of the service profile to use.</td>
</tr>
<tr>
<td>showGoalLine=value</td>
<td>Specifies whether the goal line should appear in Trend report and What-If Capacity Trend report graphs. The valid values are yes and no.</td>
</tr>
<tr>
<td>sortOrder=order</td>
<td>For a Top N report, specifies whether the report should list the elements in ascending or descending order according to the variable values. The valid values are ascending or descending. The default is descending.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject=subjectName</td>
<td>Specifies the name of the subject of the report. You can specify the name of a group, group list, or an element. When running the reports from a Distributed Console, the subjectName must follow this format: <code>machineId@elementId</code> (do not specify the actual element name). For certain reports such as Trend reports, you can specify a comma-separated list of subject names as follows: <code>subject=elemName1,elemName2</code> You cannot specify space characters in the value string.</td>
</tr>
<tr>
<td>subjectType=subject</td>
<td>Specifies the subject type for the report. The valid values are group, grouplist, and element. Refer to the Run Reports page or the Run Report dialog box to determine the valid types of subjects for each report type. For the drilldown-only reports (TopTenComponents, AllComponents, HealthIndexDetail, and SituationsTrend), you must specify element.</td>
</tr>
<tr>
<td>templateName=name</td>
<td>Specifies the name of the customized report template. You can specify a maximum of 30 single-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). Space characters are not permitted.</td>
</tr>
<tr>
<td>timeOptions=options</td>
<td>Specifies whether the report includes all hours within the specified time range, or only the hours between <code>partialDayStart</code> and <code>partialDayStop</code>. The valid values are allDay or includeHrs. The default is allDay.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeRangeType=length</code></td>
<td>Specifies the length of the report time range.</td>
</tr>
<tr>
<td></td>
<td>For a Trend report, the valid values are custom, yesterday, prev7days, thisWeek, lastWeek, thisMonth, lastMonth, prevHour, prev12Hours, prev24Hours, and prev4Weeks.</td>
</tr>
<tr>
<td></td>
<td>For an At-a-Glance report, the valid values are yesterday, todayToNow, prev7Days, thisWeek, lastWeek, thisMonth, lastMonth, prev4Weeks, prevHour, prev12Hours, prev24Hours, and custom.</td>
</tr>
<tr>
<td></td>
<td>For a Top N report, the valid values are yesterday, today, prev7days, thisWeek, and custom.</td>
</tr>
<tr>
<td></td>
<td>For a Health report, the valid values are yesterday, today, dayOf, prev7Days, lastWeek, thisMonth, lastMonth, monthEndingOn, and 7DaysEndingOn.</td>
</tr>
<tr>
<td></td>
<td>For a Service Level report, the valid values are yesterday, today, prev7Days, prev4Weeks, thisWeek, lastWeek, thisMonth, lastMonth, and custom.</td>
</tr>
<tr>
<td><code>timezone=timezone</code></td>
<td>Specifies the time zone to use for the report. The valid values are any of the eHealth internal name values (the first column) of the <code>eHealth/sys/timezone.OS.txt</code> file. The OS value represents one of the three operating systems that eHealth supports: HP, SOL, or Windows.</td>
</tr>
<tr>
<td><code>toDate=endDate</code></td>
<td>If you specify <code>timeRangeType=custom</code> or <code>timeRangeType=7DaysEndingOn</code> (Health report only), specifies the ending date for the report time range. The valid value is a date in <code>mm/dd/yyyy</code> format.</td>
</tr>
<tr>
<td><code>toDateDayOf=date</code></td>
<td>For a Health report, if you specify <code>timeRangeType=dayOf</code>, specifies the date of the day for which you want to run the report. The valid value is a date in <code>mm/dd/yyyy</code> format.</td>
</tr>
<tr>
<td><code>toDateMonthOf=date</code></td>
<td>For a Health report, if you specify <code>timeRangeType=monthEndingOn</code>, specifies the last day of the month for a monthly report. The valid value is a date in <code>mm/dd/yyyy</code> format.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>toTime=endTime</td>
<td>If you specify timeRangeType=custom, specifies the ending time for the report time range. The valid value is a time in hh:mm format with an AM or PM designation such as 11:30+PM. You cannot specify a toTime argument for Service Level reports.</td>
</tr>
<tr>
<td>topN=show</td>
<td>For a Top N report, specifies whether the report should show all values or just the top number of values. The valid values are all and top.</td>
</tr>
<tr>
<td>topNFltrDir1=direction</td>
<td>For a Top N report, specifies whether the report shows all elements in the group, or those whose variable values are above or below the specified topNFltrValN value. The valid values are all, above, and below. The default is all. Specify topNFltrDir1 for topNvar1, topNFltrDir2 for topNvar2, and so on.</td>
</tr>
<tr>
<td>topNFltrShow=show</td>
<td>For a Top N report, specifies whether the report shows elements that match all variable criteria or any of the variable criteria. The valid values are all and any. The default is all.</td>
</tr>
<tr>
<td>topNFltrVal1=value</td>
<td>For a Top N report, specifies the filtering value for each topNvarN variable. You can specify a value as a threshold against which to compare the elements. Specify topNFltrVal1 for topNvar1, topNFltrVal2 for topNvar2, and so on.</td>
</tr>
<tr>
<td>topNValue=value</td>
<td>For a Top N report, when topN=top, specifies the number of elements to show. You can specify any integer value up to 9999. The default is 20.</td>
</tr>
<tr>
<td>topNvar1=variable</td>
<td>Specifies the variables to use as the filter criteria for a Top N report. You can specify up to six filter variables. For topNvar1, you can specify the goal1, topNFltrDir1, and topNFltrVal1 arguments. For topNvar2, you can specify the goal2, topNFltrDir2, and topNFltrVal2 arguments, and so on.</td>
</tr>
</tbody>
</table>

The valid values depend on the mediumType and the group. To obtain the list of allowable variable values, use the Run Top N Report page. Specify the correct technology and group for the report. After the page refreshes, right-click in the Run Top N Report page and select View Frame Source. The HTML source lists all valid variable values. Use the string specified for each OPTION VALUE=string under the NAME=topNvarN code.
Advanced Customization of the Web User Interface

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>usePlannedDowntime=</td>
<td>For a report that includes availability charts, specifies whether to include planned downtime. The valid values are yes and no. If you do not specify a value, the default is yes. For more information, refer to the section on accounting for planned downtime in the eHealth Reports User and Administration Guide.</td>
</tr>
<tr>
<td>userVars= userVar</td>
<td>Specifies the global variables for the report using the format varname: value[,varname: value].</td>
</tr>
<tr>
<td>variable=variableName</td>
<td>For Trend reports, specifies the variables to include in the report. The valid values depend on the mediumType value. For Trend reports for a single element, you can specify a comma-separated list of variables as follows: variable=variable1,variable2 You cannot specify space characters in the value string. To obtain the list of allowable variable values, use the Run Trend Report page. Specify the correct element(s) in the Elements Selected list. After the page refreshes, right-click in the Run Trend Report page and select View Frame Source. The HTML source lists all valid variable values. Use the variable string specified for each OPTION VALUE=string under the NAME=variable code. For a Situations to Watch Detail report, specifies the Health Index threshold variable to include in the report. To obtain the Health Index variable name strings, use the daDefaults.vars file in the eHealth/reports/dataAnalysis directory. Open the file with any text editor and search for the Health Index Thresholds definition for the specified element type. Use the string specified in the thresholds definition line. An example of the syntax for the utilization definition follows: varSubLists { varSubList healthIndexThresholds { label &quot;Health Index Thresholds&quot; variables { thresholds utilization { ... webReportTitle=title</td>
</tr>
</tbody>
</table>
For the Run At-a-Glance Report page, the nhWeb program has this format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&report=reportName&reportType=glance&subjectType=subject&nameFilter=filter&mediumType=medium&subject=subjectName&granularity=sample&timeRangeType=length&fromDate=startDate&fromTime=startTime&toDate=endDate&toTime=endTime&timezone=timezone&localized=value&timeOptions=options&partialDayStart=time&partialDayStop=time&dayOptions=day&usePlannedDowntime=boolean&webReportTitle=title&webReportSubtitle=subtitle&TemplateName=name

For the Run Health Report page, the nhWeb program has this format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&report=reportName&reportType=health&subjectType=group&mediumType=medium&subject=subjectName&nameFilter=filter&timeRangeType=length&toDateDayOf=date&toDateMonthOf=date&toDate=endDate&timezone=timezone&localized=value&usePlannedDowntime=boolean&webReportTitle=title&webReportSubtitle=subtitle&TemplateName=name

For the Run Top N Report page, the nhWeb program has this format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&report=reportName&reportType=topn&subjectType=group&mediumType=medium&nameFilter=filter&subject=subjectName&topNvar1=variable&goal1=goal&topNFltrDir1=direction&topNFltrVal1=value&sortOrder=order&topNvar2=variable&goal2=goal&topNFltrDir2=direction&topNFltrVal2=value&topNvar3=variable&goal3=goal&topNFltrDir3=direction&topNFltrVal3=value&topNvar4=variable&goal4=goal&topNFltrDir4=direction&topNFltrVal4=value&show&timeRangeType=length&fromDate=startDate&fromTime=startTime&toDate=endDate&toTime=endTime&timezone=timezone&localized=value&timeOptions=options&partialDayStart=time&partialDayStop=time&dayOptions=day&usePlannedDowntime=boolean&webReportTitle=title&webReportSubtitle=subtitle&TemplateName=name

For the Run Trend Report page, the nhWeb program has this format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&report=reportName&reportType=trend&subjectType=subject&mediumType=medium&subject=subjectName&chartType=chart&divBy=divide&granularity=sample&timeRangeType=length&fromDate=startDate&fromTime=startTime&toDate=endDate&toTime=endTime&timezone=timezone&nameFilter=filter&variable=variableName&localized=value&showGoalLine=value&enableScalingPercentAxis=value&maxYValuePercentAxis=value&goalLineLabel=label&goalLineValue=value&TemplateName=name

For the Run What-if Capacity Trend Report page, the nhWeb program has this format:

http://webServerUrl/cgi-bin/nhWeb?func=runFrame&mediumType=medium&subject=subjectName&variable=variableName&chartType=chart&divBy=divide&granularity=sample&timeRangeType=length&fromDate=startDate&fromTime=startTime&toDate=endDate&toTime=endTime&timezone=timezone&nameFilter=filter&variable=variableName&localized=value&showGoalLine=value&enableScalingPercentAxis=value&maxYValuePercentAxis=value&goalLineLabel=label&goalLineValue=value&TemplateName=name&reportType=type&report=reportName&Localized=value&webReportTitle=title&webReportSubtitle=subtitle
For the Run Service Level Report page, the nhWeb program has this format:

```
http://webServerUrl/cgi-bin/nhWeb?func=runFrame&report=reportName&reportType=
  service+level&subjectType=subject&mediumType=medium&subject=subjectName&
  granularity=sample&timeRangeType=length&fromDate=startDate&toDate=endDate&
  timezone=timezone&nameFilter=filter&localized=value&usePlannedDowntime=
  boolean&webReportTitle=title&webReportSubtitle=subtitle&templateName=name
```

### Create Links to Generate Reports Automatically

You can use the nhWeb program to automatically generate a report. To create a link that generates reports automatically, you specify almost the same arguments as the link to the Run Reports page described in the previous section. However, you must specify the `func=run` and `execute=Generate+Report` arguments as follows:

```
nhWeb?func=run&execute=Generate+Report
```

For example, nhWeb uses this format to generate an At-a-Glance report:

```
  reportName&reportType=glance&subjectType=subject&mediumType=medium&subject=subjectName&
  granularity=sample&timeRangeType=length&fromDate=startDate&fromTime=startTime&
  toDate=endDate&toTime=endTime&timezone=timezone&localized=value&timeOptions=options&partialDayStart=
  time&partialDayStop=time&dayOptions=day
```

You can omit arguments such as nameFilter, which is used only to set the filter value on a Run Reports page.

### Run Report Link Examples

To create a link to run a Health report automatically, you can create an HTML HREF tag with the following format

```
  reportName&reportType=health&subjectType=group&mediumType=medium&subject=subjectName&
  timeRangeType=length&toDateDayOf=date&toDateMonthOf=date&toDate=endDate&timezone=timezone&
  localized=value" TARGET="_top">Generate a Health Report</A>
```

The following link runs a Standard Trend report:

```
  Standard&reportType=trend&subjectType=element&mediumType=ethernet&subject=
  bos-hartford-seg-1&chartType=lineStandard&divBy=time&granularity=asIs&timeRangeType=yesterday&variable=bits,bitsOut" TARGET="_top">Generate a Trend Report</A>
```

The following link runs a Health Index Detail drilldown report:

```
<A HREF="http://boston/cgi-bin/nhWeb?func=run&reportType=drildown&report=
  HealthIndexDetail&mediumType=lanWan&subjectType=element&timezone=
  &partialWeek=SMTWTFS&timeOptions=allDay&subject=192.124.15.245-SH-enet-port-1&timeRangeType=custom&serviceProfile=standard&fromDate=03/14/2000&fromTime=12:00+AM&toDate=03/14/2000&toTime=11:59+PM&execute=Generate+Report&namesType=
  names&usePlannedDowntime" TARGET="_top">Run a Health Index Detail Drill-down</A>
```
When a user clicks the link, the web server specified in webServerUrl does the following:

- Performs a security check.
- Verifies that the web user has permission to run the specified report as well as to view reports for the specified subject. If the web user does not have those permissions, the web server displays a message stating that the user does not have permission to run the report.

How to Customize the Apache Web Server

You can customize the configuration that the eHealth Apache web server uses to manage access to web reports and eHealth web pages. The httpd.conf file, which resides in the /eHealth/web/httpd directory, contains the user privileges configuration.

When you add a web user account or change some of the web user account settings, eHealth regenerates the httpd.conf file to save the new configuration changes. Therefore, if you edit the parameters in the httpd.conf file manually using a text editor, eHealth will overwrite your changes.

To customize the file, you can create a modifiable copy of the httpd.conf file named httpd.tpl and create either or both of the following protected sections within it: the Custom Basic section and the Custom Protect section. Within the Custom Basic section of the httpd.tpl file, you can define the web server configuration parameters. eHealth preserves the customized definitions in the httpd.tpl file when it regenerates the httpd.conf file by replacing the section in the httpd.conf file with those definitions from the httpd.tpl file.

To create these protected sections, you must be familiar with Apache web server protection rules. For more information about the Apache httpd configuration files, see the Apache documentation, available at http://www.apache.org.

Create the Custom Basic Section

To define web server configuration parameters, you can add the Custom Basic Section to the httpd.tpl file. Within this protected section, you can specify parameters that control the name, format, and time values for the access log file, as well as the maximum time limit for web server scripts. By including these parameters in the httpd.tpl file in a protected section, eHealth will not overwrite them when it regenerates the httpd.conf file.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerRoot</td>
<td>Specifies the server’s home directory.</td>
</tr>
<tr>
<td>User</td>
<td>On a UNIX system, sets the user ID under which the server will respond to requests.</td>
</tr>
<tr>
<td>Group</td>
<td>On a UNIX system, specifies the group ID under which the server will respond to requests.</td>
</tr>
</tbody>
</table>
Guidelines for Editing Parameters

Always use caution when changing an HTTP configuration parameter within the Custom Basic section. Do not delete any parameters from the Custom Basic section. eHealth replaces the section in httpd.conf with the Custom Basic section contained within the httpd.tpl file. If parameters are missing, the web server could malfunction.

When editing the configuration parameters for the web server, keep in mind the following:

- If you change the CustomLog parameters, they might return invalid results.
- If you specify on as the value of the HostNameLookups parameter, this setting might cause long delays in accessing any page if DNS lookup is not functioning on your system or if it is very slow.
- If you specify a value for TimeOut of less than 60 minutes, the reports that users generate from the Web might not be able to finish before the time limit expires. The reports will fail with a timeout error.

To create the Custom Basic Section within the httpd.tpl file

1. Copy the httpd.conf file to the httpd.tpl file.
2. Open httpd.tpl in any text editor.
3. Begin the section by entering the following line at the top of the file:
   
   #Custom Basic Section

4. Within the Custom Basic Section, edit the configuration parameters for the web server, but do not delete any parameters. eHealth replaces the section in the httpd.conf file with the Custom Basic Section. If parameters are missing, the web server may malfunction.

---

### Parameter Name | Parameter Description

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomLog</td>
<td>Specifies the pathname of the access log file.</td>
</tr>
<tr>
<td>ErrorLog</td>
<td>Specifies the pathname of the error log file.</td>
</tr>
<tr>
<td>HostNameLookups</td>
<td>When set to Off (the default value), the access logs use IP addresses and do not perform any DNS name resolution. When set to On, the access log entries use node names instead of IP addresses.</td>
</tr>
<tr>
<td>TimeOut</td>
<td>Specifies the maximum time limit for Web server scripts. The default is 300 seconds. You should specify a value of 300 seconds or more.</td>
</tr>
<tr>
<td>ServerType</td>
<td>Controls the way in which the Apache server handles multiple copies of itself.</td>
</tr>
</tbody>
</table>
5. End the Custom Basic Section by entering the following line immediately following
   the ScriptTimeout parameter:
   # End Custom Basic Section
   For example:
   # Custom Basic Section
   #
   ServerType standalone
   ServerRoot "C:/eHealth/web"
   #
   CustomLog httpd/httpd-log common
   ErrorLog httpd/httpd-errors
   # Timeout 300
   #
   HostNameLookups Off
   # End Custom Basic Section

6. To maintain the readability of the httpd.tpl file, delete all lines that follow the
   #End Custom Basic Section line. eHealth ignores these lines, except the
   Custom Protect Section, if you add one.

7. Save the httpd.tpl file

8. Regenerate the httpd.conf file by entering the following at the command
   line:
   eHealth/web/webCfg/nhHttpdCfg

Create the Custom Protect Section

To define web user account and directory settings, you can add the Custom
Protect Section to the httpd.tpl file. By including these parameters in the
httpd.tpl file in a protected section, eHealth will not overwrite them when it
regenerates the httpd.conf file.

To create the Custom Protect Section within the httpd.tpl file

1. Open the httpd.tpl file in any text editor.

2. Begin the section by entering the following line after the #End Custom Basic
   Section line:
   # Custom Protect Section

3. If you did not add a Custom Basic section, enter the line at the top of the
   httpd.tpl file.

4. Enter the Apache access control directives. For information on specifying
   these parameters, see the Apache documentation, available at
5. End the Custom Protect section by entering the following line after the last parameter:
   
   # End Custom Protect Section

6. Delete all lines that follow the #End Custom Protect Section line.

7. Save and close the httpd.tpl file.

8. Regenerate the httpd.conf file by entering the following at the command line:

   eHealth/web/webCfg/nhHttpdCfg

### Displaying Alias Names in eHealth

By default, eHealth displays elements with the names that it creates when it discovers them. If these names are long and difficult to recognize, you can specify more meaningful alias names. To view alias names, however, the user’s web user account must have permission to view aliases.

**To specify an alias name for an element**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage elements. The eHealth Status Summary window appears.
2. In the left pane, select Managed Resources, Elements. The element table appears.
3. Double-click the element to which you want to assign an alias. The Edit Element window appears.
4. Specify a name in the Element Alias field, and click OK. The element properties now include the alias name.

**To configure an eHealth web user account to view alias names throughout the eHealth Web user interface and the OneClickEH console interface**

1. Access the OneClickEH Console and log in to the eHealth system as a web user who has permission to view manage user accounts. The eHealth Status Summary window appears.
2. In the left pane, select Tasks and Information, User Administration. The User Administration window appears with a list of eHealth web user accounts.
3. Double-click the user account name. The Modify User window appears.
4. Select the General tab. The user account page with general account permissions appears.
5. Next to Display elements using, select Aliases, and click OK. The screen refreshes and updates the user account configuration.
To configure the eHealth console to display alias names in the eHealth console user interface

1. Log in to the eHealth console as an administrator.
   The eHealth console appears.
2. Select Setup, Options.
   The Options dialog appears.
3. Select Show Alias Names, and click OK.
   eHealth displays alias names in the Poller Configuration, Browse, Modify Element, and Add Element dialogs.

Set the Date Format in eHealth

The NH_DATE_FMT environment variable specifies the format used for the date values in eHealth reports, the eHealth console, and the web interface. This variable is set to the format that you specify during the eHealth installation. The following table shows the default settings for eHealth systems:

<table>
<thead>
<tr>
<th>Default Setting for eHealth Systems</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>MDY mm/dd/yyyy</td>
<td>31 December 2003 appears as 12/31/2003.</td>
</tr>
<tr>
<td>French and Spanish</td>
<td>DMY dd/mm/yyyy</td>
<td>31 December 2003 appears as 31/12/2003.</td>
</tr>
</tbody>
</table>

The method that you follow to change the NH_DATE_FMT environment variable varies, depending on the platform of the eHealth system.

To set NH_DATE_FMT on a Windows system

1. Modify NH_DATE_FMT by following the procedure outlined in Setting Environment Variables on Windows Systems in the eHealth Help for environment variables. Change the value to one of the following:
   - MDY mm/dd/yyyy
   - DMY dd/mm/yyyy
   - YMD yyyy/mm/dd
2. Propagate the change to the eHealth Web user interface by following the standard procedure for rebooting the system.
   The web server now uses the updated date format.
To set NH_DATE_FMT on a UNIX system

1. Modify NH_DATE_FMT by following the procedure outlined in Setting Environment Variables on UNIX Systems in the eHealth Help for environment variables. Change the value to one of the following:
   - MDY  \textit{mm/dd/yyyy}
   - DMY  \textit{dd/mm/yyyy}
   - YMD  \textit{yyyy/mm/dd}

2. Propagate the change to the eHealth Web user interface by doing one of the following:
   - On Solaris, open the /etc/init.d/httpd file, update the value of NH_DATE_FMT, and save the file.
     The Web server now displays the updated date format.
   - On HP-UX, open the /sbin/init.d/httpd file, update the value of NH_DATE_FMT, and save the file.
     The Web server now displays the updated date format.

3. Log in as the eHealth user, and enter the following commands at a command prompt:
   - \texttt{nhHttpd stop}
   - \texttt{nhHttpd start}
   The eHealth server stops and restarts. The Web server now displays the updated date format.

Set the Time Format in eHealth

The NH_TIME_FMT environment variable specifies the format used for the time values in eHealth reports, the eHealth console, and the web interface. This variable is set to the format that you specify during the eHealth installation. The following table shows the default settings for eHealth systems:

<table>
<thead>
<tr>
<th>Default Setting for eHealth Systems</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>English and Japanese</td>
<td>12Hour indicates a 12-hour clock that includes AM or PM designations</td>
<td>8:30 PM is specified as 8:30 PM</td>
</tr>
<tr>
<td>French and Spanish</td>
<td>24Hour indicates a 24-hour (military-style) clock.</td>
<td>8:30 PM is specified as 20:30</td>
</tr>
</tbody>
</table>

\textbf{Note:} On French and Spanish eHealth systems, you cannot change the time format to use a 12-hour clock; that is, you cannot define NH_TIME_FMT as 12Hour.
The method that you follow to change the NH_TIME_FMT environment variable varies, depending on the platform of the eHealth system.

**To set NH_TIME_FMT on a Japanese or English Windows system**

1. Modify NH_TIME_FMT by following the procedure outlined in Setting Environment Variables on Windows Systems in the eHealth Help for environment variables. Change the value to 24Hour.
2. Propagate the change to the eHealth Web user interface by following the standard procedure for rebooting the system.
   - The web server now uses the updated time format.

**To set NH_TIME_FMT on a UNIX system**

1. Modify NH_TIME_FMT by following the procedure outlined in Setting Environment Variables on UNIX Systems in the eHealth Help for environment variables. Change the value to 24Hour.
2. Propagate the change to the eHealth Web user interface by doing one of the following:
   - On Solaris, open the /etc/init.d/httpd file, update the value of NH_TIME_FMT, and save the file.
   - The web server now uses the updated time format.
   - On HP-UX, open the /sbin/init.d/httpd file, update the value of NH_TIME_FMT, and save the file.
   - The web server now uses the updated time format.
3. Log in as the eHealth user, and enter the following commands at a command prompt:
   - nhHttpd stop
   - nhHttpd start
   - The eHealth server stops and restarts. The web server now uses the updated time format.

**Specify Date and Time Preferences for the OneClick for eHealth Interface**

By default, OneClickEH displays dates using the YYYY-MM-DD weekday format and displays time using the hr:minute:second PM/AM format. You can specify your own preferences for the default format of dates and times that appear throughout your OneClickEH interface.

**To specify your date and time preferences**

1. Select Tools, Options in the menu bar.
2. In the left pane of the Options dialog, click the Date/Time icon
3. (Optional) Select a different date format and/or a different time format from each list.
4. (Optional) Do one or both of the following under Date and Time Format:
   - Specify that the date appear before the time. Select Date First, select a format from the date list, and select a format from the time list.
   - Specify that the time appear before the date. Select Time First, select a format from the time list, and select a format from the date list.

5. Click Apply, and then click OK.

**Customize the User Administration Screen of the OneClick for eHealth Interface**

The User Administration screen displays a summary of permissions for each user account to enable you to quickly identify the users who have permission to perform a particular action. By default, OneClickEH displays three columns: OneClickEH Access, Group Access, and Group List Access. You can easily customize the screen to display more permissions by using the field-chooser feature.

**To customize the screen**

1. Right-click a column header.
2. Select Select Fields. In the Select Fields dialog, select all column names or specific column names that you want to display and click Add. You can quickly add individual names to the list by double-clicking them.
3. Double-click to remove any columns that you do not want to display.
4. Use the Move Up and Move Down buttons to reorder the list of column headers.
5. Click OK.
6. After the User Administration screen refreshes, use your mouse to drag and drop columns to rearrange them in the order in which you would like to view them.

**Customize OneClickEH Tables**

By default, OneClickEH displays a standard set of columns in each element table. You can customize each of your tables by using the field chooser feature.

**To customize a table**

1. Right-click a column header or any element in the table.
2. Select Select Fields.
3. In the Select Fields dialog, select one or more column names that you want to include and click Add.
4. Remove any columns that you no longer want to display.
5. Use the Move Up and Move Down buttons to reorder the list of column headers.
6. Click OK.
Save OneClickEH Table Entries

To save some or all of the data in a OneClickEH table, you can perform any of these actions by right-clicking in the table or selecting the table icon at the top of the screen under the Actions menu:

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all entries in the table.</td>
<td>Place your cursor inside the table, right-click, and select Select All.</td>
</tr>
<tr>
<td>Copy selected entries in the table to a file.</td>
<td>Use Ctrl on your keyboard to select two or more entries individually (or use Shift to select two rows and all rows between them). Right-click and select Copy. Paste the data into a file and save it. (You can also drag and drop selected entries to another application.)</td>
</tr>
<tr>
<td>Export selected entries in the table to a file.</td>
<td>Use Ctrl on your keyboard to select two or more entries individually (or use Shift to select two rows and all rows between them). Right-click and select Export Selected. Save the data to the comma-separated value (.csv) file.</td>
</tr>
<tr>
<td>Export the entire table to a file.</td>
<td>Right-click and select Export All. Save the data to the .csv file.</td>
</tr>
<tr>
<td>Print the entire table.</td>
<td>Right-click and select Print.</td>
</tr>
</tbody>
</table>
Appendix F: Troubleshooting and Best Practices for Administering eHealth

Create Technical Support Information

If you experience any problems or errors while using the eHealth products and features, Support may direct you to create a troubleshooting Zip file that can help them to diagnose the problem. You must be logged in as the eHealth web administrator to create these files.

**Important!** Depending upon the options that you select, the troubleshooting Zip file could be very large. Typical Zip files can range in size from 50 KB to 150 MB. If you have had Advanced Logging enabled for a long time, the Zip file may be several Gigabytes in size.

**To create a troubleshooting Zip file**

1.  [Log In to the eHealth Web User Interface](#) as an administrator.
   The Administration page appears.
2.  Click the Administration tab on the navigation bar.
   The Administration page appears.
3.  In the left frame, click eHealth Management, Advanced Logging.
   The Advanced Logging page appears.
4.  (Optional) If your Support engineer directs you to enable advanced logging before creating the troubleshooting Zip file, follow the instructions in [Enable Advanced Logging for Web Server Processes on page 270](#) to create the logs.
5.  Click Advanced Logging in the left pane to redisplay the Advanced Logging page, and then Click Create Technical Support Information.
   The Create Technical Support Information page appears.
6.  Do the following and then click Create File:
   a.  Under Areas to Include, select one or more areas as instructed by your Technical Support Engineer.
b. (Optional) If your eHealth system is a member of a Distributed eHealth cluster, in the Cluster Members field, do one of the following:
   - Select Host to specify the cluster member for which you want to collect troubleshooting information. The default is the local cluster member.
   - Select Cluster to collect the same information from all cluster members except the local member.
   - Select All to collect the same information from all cluster members.

c. In the File Directory field, specify the directory in which to create the Zip file. The default is /eHealth/tmp.

d. In the Call Ticket Number field, specify the number of the call ticket for your problem report. If specified, the number is used in the Zip file name for identification purposes. If you do not have a call ticket associated with this problem, leave the field blank.

   The tool collects copies of files from various subdirectories of the eHealth installation and creates a Zip file named diagnostics_callTicketNumber_date_time.zip in the specified File Directory location.

7. Email or FTP the Zip file to Support to assist with the process of troubleshooting the problem that you have reported.

   Support will confirm that they have received the file.

8. Delete the Zip file from your File Directory location.

   eHealth frees the system disk space.

Enable Advanced Logging for Web Server Processes

To troubleshoot and debug certain types of problems that can occur with the eHealth web software, Technical Support may require you to enable advanced logging prior to creating the troubleshooting Zip file. As a best practice, do not enable advanced logging unless you are troubleshooting a specific problem under the direction of Support or your Sales Engineer. To access this feature, you must log in through the eHealth Web user interface as the web admin.

To use advanced logging through the eHealth Web user interface

1. Log In to the eHealth Web User Interface as an administrator.
   
   The Administration page appears.

2. Select eHealth Management, Advanced Logging.
   
   The Advanced Logging page appears.

3. Specify the web user for whom you want to generate logs, the web pages, and the time range; then click Apply.
   
   eHealth stores the log files in the /eHealth/log/advanced directory.
Enable Advanced Logging for eHealth System Processes

To resolve certain types of eHealth system process problems, Technical Support may require you to enable advanced logging prior to creating the troubleshooting Zip file. Some of these options can interfere with your system performance, and most of the log files consume a significant amount of disk space. As a best practice, do not enable advanced logging unless you are troubleshooting a specific problem under the direction of Support or your Sales Engineer. To access this feature, you must log in to the OneClick for eHealth console as a web user who has permission to manage advanced logging.

To use advanced logging through the OneClickEH console

1. Log in to the OneClick for eHealth console by entering the following in a web browser, where eHealthSystem is the specific name of the system on which eHealth is installed. If your eHealth system is configured to run in a High Availability environment, specify the shared IP address or shared hostname for your system rather than the specific eHealth system name.

   eHealthSystem/OneClickEH

   The Connect to eHealthSystemName window appears.

2. Specify a user name and password of an administrator who has permission to access OneClickEH; then click OK.

   The OneClick for eHealth page appears.

3. Click Launch OneClick for eHealth.

   The File Download window appears.

4. Click Run.

   The OneClickEH login window appears.

5. Specify the user name and password of an administrator who has permission to manage advanced logging; then click Log In.

   The eHealth Status Summary window appears.

6. In the left pane of the console, click Tasks and Information, Setup; then click Advanced Logging.

   The Advanced Logging window appears.

7. Select the tasks for which you want to access eHealth log files; then click Apply and View Advanced Logs.

   Important! Because most of these log files can consume a significant amount of disk space, some of the options available in the Advanced Logging window can interfere with your system performance. Select these options under the explicit direction of Technical Support.

8. OneClickEH automatically opens the Server Files folder and displays the log files pertaining to the tasks. Press the F5 key, if necessary, to refresh the directory listing.
Advanced Logging Tool Creates an Incomplete Zip File

Valid on Windows and UNIX

Symptom:

The Advanced Logging troubleshooting tool creates an incomplete Zip file.

Solution:

For each troubleshooting option, the tool searches for each file and then checks for available space in the File Directory location. If it cannot find a specific file, or if File Directory does not have enough free space to hold a file, the tool omits that file and proceeds to the next one. The Zip file contains a log file that lists the files that were included, as well as those files that were omitted. If any files were omitted, confirm that the File Directory has enough free space to accommodate the files, and confirm that the files are exist.

Devices Lose Data before eHealth Can Collect It

Valid on Windows and UNIX

Symptom:

If poll intervals are too long, you have a complex polling environment, or your element configuration grows significantly, the devices may lose data or discard it before eHealth can collect it from them. If this problem occurs, eHealth displays messages indicating that a poll was missed.

Solution:

As a best practice, tune your statistics poller after your configuration grows so that the poller operates more efficiently. This reduces the SNMP polling impact on shared system resources and allows the eHealth installation to maximize its element configuration size. For instructions, see the Tuning the eHealth Statistics Poller White Paper, which is available on the Support web site.
Discover Log Reports Several Suspected Duplicates

Valid on Windows and UNIX

Symptom:

Suspected duplicate elements occur when you save the results of a discover process that include a change in an index value of an element that eHealth cannot track with a discover key. Systems and system agents are very dynamic. On some systems, element indexes can change as a result of inserting a CD-ROM into a drive. Router interface elements can change indices when the router reboots, a card is inserted or removed, or when you install firmware upgrades.

Solution:

Regularly update the original element with its current index value.

eHealth Web Server Is Inaccessible on a Windows System

Valid on Windows

Symptom:

You are unable to access the eHealth web server on a Windows system through a web browser.

Solution:

The server may have stopped. You must use your Windows control panel to start it manually when you want to access it.

Start Apache Web Server Manually on Windows System

eHealth automatically installs the Apache web server and software to allow you to view reports from a web browser. You can access the eHealth web server by specifying the server’s URL in a web browser (http://ipAddress). If you are unable to access the web server, the server may have stopped. You must start it manually when you want to access it.
To start the Apache web server manually

1. Select Start, Settings, Control Panel. The Control Panel window appears.
4. Select eHealth httpdnn; then click Start. The number of the current eHealth release is appended to the name of the eHealth Windows service.
5. Click Close. The Services window closes, and the Apache web server starts.

eHealth Web Server Is Inaccessible on a UNIX System

Valid on UNIX

Symptom:

You are unable to access the eHealth web server on a UNIX system.

Solution:

The server may have stopped. You must start it manually when you want to access it.

Start Apache Web Server Manually on UNIX System

eHealth automatically installs the Apache web server and software to allow you to view reports from a web browser. You can access the eHealth web server by specifying the server’s URL in a web browser (http://ipAddress). If you are unable to access the web server, the server may have stopped. You must start it manually when you want to access it.

To start the Apache web server manually on a UNIX system

1. In a terminal window, log in as the root user:
2. Do one of the following:
   - On a Solaris system, enter the following:
     `/etc/init.d/http start`
   - On an HPUX system, enter the following:
     `/sbin/init.d/httpd start`
   For information on using the Apache web server, see the eHealth Installation Guide for your platform.

---

**eHealth Generates Error after Changing Date or System Time**

**Valid on Windows**

**Symptom:**

If you move the month forward on a Windows system, eHealth uses that new time when recording any data that it polls during this temporary time change. If you exit the window by cancelling, thereby reverting to the previous time, eHealth tries to enter subsequent data earlier than your last entry. The database does not allow this action, so it results in an error.

**Solution:**

If you have a Windows system and you need to change your system date or time when eHealth is running—even temporarily—use caution. If you must do so, stop the eHealth server first, change the date or time, and then restart the server. Your reports will show a gap in data while the server is stopped.

---

**OneClickEH Installation Fails**

**Valid on Windows**

**Symptom:**

If you attempt to install OneClickEH on a Windows system on which you are running a virus scanner, the installation might fail or experience problems.

**Solution:**

Before you install OneClickEH, disable the virus scanner on your system. After the installation finishes, re-enable the scanner.
Statistics Polling Errors Remain after Being Resolved

Valid on Windows

Symptom:

After you resolve all errors of a particular type using the pop-up menu, the World View does not automatically refresh the Polling Management folder by removing that error type from the folder.

Solution:

You must left-click the folder to update the tree display. If you do not generate errors of a particular type during the next normal poll, that error type will no longer appear in the tree under Polling Management. After the next poll, the World View updates automatically to reflect the changes.

Poll Durations Are at or near the Normal Polling Interval

Valid on Windows and UNIX

Symptom:

You observe that the poll durations for many of your elements are at or near the normal polling interval.

Solution:

Your eHealth configuration may have grown considerably. To make sure that the poller operates efficiently and puts less strain on shared system resources, and to enable eHealth to maximize its element configuration size, consider tuning your poller. For instructions, see the Tuning the eHealth Statistics Poller White Paper, which is available on the Support web site.
Some Elements Are Not Selectable in the Element Tables

Valid on Windows

Symptom:
Retired elements and any elements that eHealth is polling on a remote site appear grayed-out in all element tables and you cannot perform any element actions on them.

Solution:
You cannot use OneClickEH to manage retired elements and any elements that eHealth is polling on a remote site. To manage a retired element, right-click it and select Unretire. To manage a remotely polled element, log in to the remote polling site in your OneClickEH World View.

Able to Log In to OneClickEH without Supplying a Password

Valid on Windows

Symptom:
After the user click Launch OneClick for eHealth, the Login window appears, but the system automatically supplies the password and displays the World View without requiring the user to log in to the system.

Solution:
By default, OneClickEH requires every user to supply a web user name and password to log in to an eHealth system. After a user logs in, OneClickEH displays a dialog to allow the user to save the login information. Once OneClickEH saves login information for a system, it automatically supplies the user name and password for every future login attempt. Disable the automatic login or change an eHealth system configuration file to prevent users from being able to use it.
Disable the Automatic Login for an eHealth System

After a OneClickEH user saves login information for a system, OneClickEH automatically supplies the user name and password for every future login attempt. You can disable the automatic login by changing an Advanced Setting.

To disable the automatic login for an eHealth system

1. Log In to the eHealth Web User Interface.
2. In the left pane, select Launch OneClick for eHealth. The File Download window appears.
3. Click Open. The OneClickEH Login window appears.
4. Log in to the eHealth server as an administrator who has permission to manage user accounts. The eHealth Status Summary window appears.
5. Right-click the World View icon in the tree and select Other Options, or select Tools, Options, Advanced. The Advanced Settings window appears.
6. Do the following, and then click OK:
   - Deselect the appropriate options to disable the automatic login.
   - (Optional) Clear all temporary objects that you have saved during your OneClickEH session.

   The Advanced Settings window closes.
7. Log out of the system and then log in again. OneClickEH now requires you to supply the user name and password.

Hide the Login Save Feature from a OneClickEH User

After a OneClickEH user saves login information for a system, OneClickEH automatically supplies the user name and password for every future login attempt. You can hide the login save feature from a user by changing a configuration file.

To hide the login save feature from a user

1. Select Start, Run. The Run window appears.
2. Specify cmd in the Open field and click OK. A command prompt window appears.
3. Log in to the eHealth system as an administrator and do the following.
   a. Change directories to `eHealth/web/cmi.usr/config`.
   b. Create a file named `cmi.ini` within this directory.
   c. Add the following text to the file:

   ```
   server-options=[HIDE_REMEMBER_LOGIN]
   ```

   d. Save and close the file.

   OneClickEH hides the user name and password prompts in the Advanced Settings window and no longer prompts the user to save the login information after every login attempt.

---

**Fail to Discover a PVC for an ATM Probe**

*Valid on Windows and UNIX*

**Symptom:**

When you attempt to discover a PVC for an ATM probe, eHealth returns an error indicating that the device does not exist.

**Solution:**

You may be trying to discover devices that are not certified. Navigate to the Certified Devices page on the product Web site to determine if the devices are fully certified.

---

**Fail to Discover Multiple Routers with Channels**

*Valid on Windows and UNIX*

**Symptom:**

When you attempt to discover multiple routers with channels, eHealth returns an error indicating that the routers do not exist.

**Solution:**

You may be trying to discover router devices that are not certified. Navigate to the Certified Devices page on the product Web site to determine if the routers are fully certified.
Unable to Identify SNMP Agents That Allow eHealth to Discover Systems

Valid on Windows and UNIX

Symptom:

You are unable to identify which agents will allow eHealth to discover systems.

Solution:

You may be trying to discover systems that are not certified. Navigate to the Certified Devices page on the product Web site to determine if the systems are fully certified.

Unable to Determine Which Systems to Poll

Valid on Windows and UNIX

Symptom:

You are unable to identify which systems that you need to poll.

Solution:

You may be trying to discover systems that are not certified. Navigate to the Certified Devices page on the product Web site to determine if the systems are fully certified.
Encounter a Fatal Error on a UNIX System after a Discover

Valid on Windows and UNIX

Symptom:

If you receive a fatal error in the eHealth console system messages window after attempting to perform a discover.

Solution:

Another user may have reset the ownership and permissions of one or more eHealth core files. Verify that the ownership and permissions of these files are set to root.

Change Ownership of eHealth Files to Root

To perform all eHealth functions such as discover, you must own the following core eHealth files: nhiDiscover, nhiPoller, and nhiTrapServerCmu. All files must be owned by the root user.

To change the ownership of eHealth files to root

1. Log in to a UNIX eHealth system as any valid UNIX user account and open a command/shell window.
2. Change to the eHealth home directory.
3. Change to the following directory:
   ```
   cd /opt/eHealth
   ```
4. Set the eHealth environment variables for your command session.
   ```
   source nethealthrc.csh
   ```
5. Change to the eHealth directory in which these internal commands reside.
   ```
   cd bin/sys
   ```
6. Enter the following to display the full output of each file, where `fileName` is nhiDiscover, nhiPoller, or nhiTrapServerCmu:
   ```
   ls -al fileName
   ```
   The command should display output similar to the following:
   ```
   -r-sr-xr-x 1 root doc 1154740 Sep 20 05:40 fileName
   ```
7. If the owner of any of the files is *not* root, change the owner and the permissions on the file to root by doing the following:
   a. Enter the following command:
      
      `chown root fileName`
   
   b. If the permissions bits for the file do not match the string shown in Step 6, enter the following command to reset them:
      
      `chmod u+s fileName`

8. Repeat Steps (a) and (b) to change the permissions of the other files, if necessary.

   You should now be able to perform core eHealth functions such as discovery without encountering fatal errors.

**Unable to Discover Gigabit Ethernet Interfaces on a System**

Valid on Windows and UNIX

**Symptom:**

When eHealth discovers gigabit Ethernet interfaces on a system, they appear in the user interface as LAN or WAN elements. eHealth does not recognize the gigabit Ethernet interface description, so it assigns a description of MIB2 (WAN port) to it by default. As a result, you cannot discover the interface on the system.

**Solution:**

To make sure that these elements appear as system elements in a report, do one of the following:

- Submit a certification request to certify the interfaces.
- Use the Poller Configuration dialog to change the agent type of the element from MIB2 (WAN port) to MIB2 (LAN port).
- Use the OneClick for eHealth console to change the speed to one gigabit and assign the system as the parent object.
- Contact CA Technology Services to request assistance in modifying your version of eHealth.
Unable to Perform a Discovery for a Particular Technology

Valid on Windows and UNIX

Symptom:

You are unable to perform a discovery for a particular technology.

Solution:

Use OneClickEH to confirm that the appropriate license is present and has not expired.

Unable to Save Data for an Element in the Database

Valid on Windows and UNIX

Symptom:

You run a report for an element and the generated reports are blank. The database does not contain any data for the element. The setting of the ifOperStatus field is set to down.

Solution:

Although eHealth can discover an element that is unavailable, it does not save data for an element in the database until the device becomes available and the setting of the ifOperStatus field changes to up. For example, if you discover a router, eHealth discovers all of the interfaces configured on that router, regardless of their availability status. To enable eHealth to save data for the elements, you must set the ifOperStatus field to up. For instructions, see the chapter on creating a MIB translation file (MTF) in the eHealth Customizing Variables Administration Guide.
Receive Incorrect Line Speeds on Devices after Discovery

Valid on Windows and UNIX

Symptom:

You encounter incorrect line speeds on devices after you discover them.

Solution:

You must modify the elements to use the correct speed.

Reporting No Data for New Variables

Valid on Windows and UNIX

Symptom:

After upgrading to a new release of eHealth and then performing a discovery, the database does not contain the new variables.

Solution:

When you upgrade to a new release of eHealth, you should rediscover elements to update them for any changes, such as new variables that are available. If you do not rediscover the elements, your database will not have this information. If a variable has changed, eHealth updates the elements after you perform a discovery on them.
Discovered Different Agent Types for One Element

Valid on Windows and UNIX

Symptom:

The discover process creates interface elements that are children of a parent for aggregate statistics using one agent type, and also creates interface elements for individual port statistics with another agent type.

Solution:

An element can have two different agent types if you discover a device using multiple technologies. This is normal eHealth functionality. You must decide how you would like to manage your devices, and only discover these dual-approach agents using one technology.

Unable to Poll and Report on ATM Ports, Paths, and Channels

Valid on Windows and UNIX

Symptom:

You cannot poll or report on ATM ports, paths, and channels.

Solution:

eHealth defines WAN links, including those used for ATM or to carry Frame Relay PVCs, as WAN elements. However, to poll and report on ATM ports, paths, and channels, you must have an eHealth – ATM license; to poll Frame Relay PVCs, you must have an eHealth – Frame Relay license. After you add these licenses (if they are not already in your license.dat file), you must run discover again.
Unable to Send Scheduled Discover Results to Multiple Recipients

Valid on Windows and UNIX

Symptom:

You receive an error after trying to send scheduled discover results to multiple recipients by including spaces in the list.

Solution:

To send scheduled discover results to multiple recipients, do not use the same method that you would use to send reports to multiple people. You must enter all e-mail addresses in the Notify User field of the Add Scheduled Discover Jobs dialog, and separate each one with a comma. Do not use spaces.

Unable to View Elements after Specifying a Group Name

Valid on Windows and UNIX

Symptom:

You are unable to view elements that you discovered using the Save to (group) option in the Create Discover Policy window.

Solution:

You must use the Options dialog to change the element filter to the group name.
Unable to Discover the Speed of Elements

Valid on Windows and UNIX

Symptom:

When you discover ATM elements, eHealth does not discover the Speed Out variable and automatically update the committed information rate (CIR) speed for the devices.

Solution:

When discovering ATM elements, eHealth discovers the Speed Out variable if it is included in the device MIB. If you change the CIR speed on a router, eHealth does not automatically update it; you must rediscover that device.

Discovering RAS Devices as Router Elements

Valid on Windows and UNIX

Symptom:

When discovering routers, eHealth discovers remote access server (RAS) devices as router elements, and then includes the RAS in router reports, but not in RAS reports.

Solution:

Because RAS devices perform routing services, the discover process for routers could discover RAS devices as router elements. Manage your RAS devices using the eHealth — Remote Access Server license—not a Router license. If you choose to report on a RAS as both a router element and a RAS element, eHealth polls the RAS device and its elements twice.
Unable to Collect Alternate Latency Information or Data from Response Sources

Valid on Windows and UNIX

Symptom:

You are unable to collect alternate latency information or data from response sources.

Solution:

Specify a community string that gives you read and write access to the element when you discover or modify its information in the database.

Unable to Exclude Data for Remotely Mounted Partitions

Valid on Windows and UNIX

Symptom:

Data for remotely-mounted partitions appears in system reports.

Solution:

To exclude data for remotely-mounted partitions, drives, or volumes from your report, disable polling for the remote partitions. If you delete the remote partitions, eHealth will rediscover them the next time that it discovers the system.
Unable to Create Process Set Elements for a System

Valid on Windows and UNIX

Symptom:

You are unable to create process set elements for systems.

Solution:

eHealth creates process set elements and process elements for a system if the system has a system agent and if the application running on that system is defined in the process definition file. eHealth can only poll process elements for a system for which you have specified a community string that has read-write permissions. For more information, see Chapter 10: Managing and Monitoring Systems.

Unable to Discover Sun/System Token Ring Interfaces

Valid on Windows and UNIX

Symptom:

When you discover token ring interfaces using the System technology, eHealth discovers them as MIB2 LAN elements and reports generic statistics.

Solution:

To obtain true token ring specifics, you must discover the interface using the LAN/WAN technology.
Receive Incorrect Statistics When Rediscovering Lite Switches

Valid on Windows and UNIX

Symptom:

If you do not delete the Lite switch from the database before rediscovering it, eHealth includes the Lite backplane by aggregating the statistics from the interfaces and the backplane, which results in inflated total statistics for the switch.

Solution:

Likewise, before rediscovering an existing traditional or Plus switch element as a Lite switch, you must delete it.

Unable to Track Data for an Element during Link Change from One Router to Another

Valid on Windows and UNIX

Symptom:

Sometimes eHealth cannot seamlessly track the data for an element during a change. If the element type changes, such as from a token ring interface to an FDDI interface, eHealth cannot use one element to track both types of data.

Solution:

You must retire the old element and create a new element for the new element type.
Double Polling Routers That Are Also Systems

Valid on Windows and UNIX

Symptom:
If you run discover for both the Router and System technologies, eHealth discovers elements that are both routers and systems twice: once as router elements, and once as system elements. eHealth also polls those elements twice.

Solution:
You can retire one of the elements to prevent double polling of the same element. As a best practice, limit your discovery of elements that could be discovered as both systems and routers to the technology in which you are interested. If you want to save detail data on the interfaces to the database for reporting, discover the elements using either the LAN/WAN and System technologies or the LAN/WAN and Router technologies, but not in all three. If you are not concerned with detailed data but want to run System reports or Router reports, run discover using Router and System technologies, but not using the LAN/WAN technology.

eHealth Misses a Scheduled Poll

Valid on Windows and UNIX

Symptom:
eHealth displays the following message in the console when the next poll was scheduled to occur:

A scheduled poll was missed, the next poll will occur now.

Solution:
If polls are taking longer than the specified polling interval, the poller might be busy or is processing a configuration update. If you receive this message every time the poller runs, consider doing one of the following:

- Use a longer polling interval.
- Tune the poller settings.
- Consider upgrading the eHealth system to a higher performing system if the system is under-powered.
Unable to Report on Router Interface Elements

Valid on Windows and UNIX

Symptom:

eHealth does not save detailed performance data on router interface elements when you discover them using the Router/Switch Discovery technology. It aggregates the data for those interfaces to the total data for the router. As a result, you cannot run LAN/WAN reports on the router interface elements.

Solution:

You must discover the router using the LAN/WAN technology or modify the interface element to record detail data.

eHealth Reports the Speed of Elements as Zero

Valid on Windows and UNIX

Symptom:

A device reports its speed as zero, and eHealth does not change the speed setting.

Solution:

eHealth checks the speed of LAN elements and full-duplex interface elements at every poll. If the device is not configured properly and reports the speed as zero, eHealth does not change the speed settings. As a best practice, make sure that your element speeds are correct. If they are not, reports on bandwidth utilization could report incorrect data. If the speeds are not configured correctly, eHealth sets the default speed values to those values that it polls from the device. To set the correct speeds, double-click the elements in the OneClick for eHealth console, select the Speed tab, change the values, and click OK.
Web Server Response Time Is Slow

Valid on Windows and UNIX

Symptom:

The response time for the eHealth web server is slow.

Solution:

You can improve web server response time on any system from which you access the web server by using a text editor (such as Notepad) to add the IP address and name of the eHealth system to the hosts file. On Windows systems, the hosts file is in the /winnt/system32/drivers/etc/ directory. On UNIX systems, the file is in the /etc directory.

HTML Help Modifications Lost after Upgrade

Valid on Windows and UNIX

Symptom:

After upgrading, all modifications that you made to HTML Help pages are overwritten.

Solution:

If you modify existing eHealth Help pages, you will lose the changes the next time that you upgrade eHealth because the upgrade process overwrites your files. Before you upgrade, place a copy of your modified files in a protected directory such as /eHealth/web/help/custom so that you can replace the files after you upgrade.
Cannot Create Links to Pages and Reports

Valid on Windows and UNIX

Symptom:

You encountered an error after using nhWeb to create links to pages and reports.

Solution:

If you encounter an error when using nhWeb in HTML HREF or http://links, you may have included space characters, carriage returns, or new lines within the nhWeb program string. To resolve the error, search the string and replace any required spaces in variable names or other values with the plus (+) character or %20. Also, remove any carriage returns and newlines.

Cannot Display a Tabbed Page

Valid on Windows and UNIX

Symptom:

One or more tabbed pages do not appear in your eHealth Web user interface.

Solution:

If you are unable to display a tabbed page in the web interface, your web server domain name may have changed, which resulted in a broken link. To make sure that your custom links function correctly, omit http://webServerUrl for links that you specify in pages that are local to the web server; that is, pages that reside in the /eHealth/web/output directory. If your web server domain name changes for any reason, your custom links will then still function correctly.
Web Browser Replaces Frame Where Link Appeared Only

Valid on Windows and UNIX

Symptom:

You are unable to display a page that has a link to nhWeb.

Solution:

the page may be part of a frameset. You may have to include the TARGET="_top" in your HTML code so that the web browser replaces the entire browser window with the new page. Otherwise, the web browser replaces only the frame in which the link appeared. For example:

<A HREF="http://miami/cgi-bin/nhWeb?func=adminFrame" TARGET="_top"> Go to Administration Page</A>

When you click the link, the web server performs a security check.

Report List Filters Do Not Show All Groups

Valid on Windows and UNIX

Symptom:

All of your groups do not appear on the Report List page of your eHealth Web user interface.

Solution:

When you create nhWeb links to the Organization and Report List pages, you can select the report list filter values to customize and control the default report list for your Web users; however, the filters will show only those reports for the groups, group lists, and elements that the web user account is permitted to view. To set access permissions for Web users, use the User Administration feature of the OneClickEH console.
Web Server Malfunctions

Valid on Windows and UNIX

Symptom:

Your eHealth web server has malfunctioned.

Solution:

You or another eHealth administrator may have deleted some parameters from the Custom Basic Section of the httpd.conf file. The httpd.conf file, which resides in the eHealth/web/httpd directory, contains the security and privileges configuration for the eHealth Apache web server. Do not delete any parameters from the Custom Basic Section. eHealth replaces the section in the httpd.conf file with the Custom Basic Section contained within the httpd.conf file. If parameters are missing, replace them in the file and save it.

Unable to Start Apache Web Server

Valid on Windows and UNIX

Symptom:

The Apache Web server will not start automatically.

Solution:

If the Apache web server will not start, do any or all of the following:

- Check the system application log file to obtain information about the cause.
- Check the web server error log in the eHealth/web/httpd/httpd-errors file.
- Check the ServerName setting in the eHealth/web/httpd/httpd.conf file.
- Start it manually.
Reports Fail with a Timeout Error

Valid on Windows and UNIX

Symptom:

A web user’s report fails with a timeout error.

Solution:

Check the Custom Basic Section of the httpd.tpl file to confirm that the value of the TimeOut web server configuration parameter is 60 minutes or more. The TimeOut web server configuration parameter specifies the maximum time limit for Web server scripts. If you specify a value of less than 60 minutes, the reports that users generate from the web might not be able to finish before the time limit expires. The reports will then fail with a timeout error. To correct the error, modify this parameter in the Custom Basic Section of the httpd.tpl file.

Experiencing Long Delays in Accessing Pages

Valid on Windows and UNIX

Symptom:

A web user experiences long delays in accessing web pages.

Solution:

When the HostNameLookups configuration parameter in the Custom Basic Section of the httpd.tpl file is set to Off (the default value), the access logs use IP addresses and do not perform DNS name resolution. When it is set to On, the access log entries use node names instead of IP addresses. If DNS lookup is not functioning on the Web user’s system or it is very slow, setting this parameter to On may prevent access to certain pages. To correct the problem, you may have to change the setting of the HostNameLookups configuration parameter.
nhWebProtocol Generates Errors

The nhWebProtocol command logs errors when command-line arguments are invalid, or specified certificates or keys are missing. To troubleshoot these errors, see the Apache error log file created in eHealth/web/httpd.

SSL Connection Fails

If you enable SSL and the command appears successful but the SSL connection fails, confirm that you have not chosen a port that is currently being used.

If you disable SSL on a server and then attempt to log on to an eHealth web interface using HTTPS in the web address, the connection fails. Both the eHealth server and client must use HTTP or HTTPS, but they cannot use both protocols at once.

If you have trouble connecting to a system that is SSL enabled, verify that the eHealth system hostname you are using matches the hostname you specified when you generated the CSR and private key. If the SSL connection fails:

- Confirm that the HTTPS or the Use Secure Connection option is selected from the eHealth client application (Live Health, OneClick for eHealth, Report Center, etc.).
- Try restarting Apache by doing the following:
  - (UNIX) From a CLI enter the following commands:
    nhHttpd -stop
    nhHttpd -start
  - (Windows) Open Control Panel, Administration Tools, Services. In the Services window, stop and re-start the following services:
    eHealth httpd60
    eHealth tomcat60

Syntax Failure

Reason

Incorrect syntax was entered when specifying the nhWebProtocol arguments.

Action

Confirm that you have entered the correct hostname, certificate name, or key name and run the nhWebProtocol command again.
SSL Connection Fails

Log In Failure

Reason
Invalid user name or password was used while logging in to an eHealth web user interface.

Action
Verify that you are using the correct user name or password and try logging in again.

Certificate File Does Not Exist

Reason
An invalid or nonexistent certificate file was entered.

Action
Confirm that you are using a valid certificate file.

Key File Does Not Exist

Reason
An invalid or nonexistent key file was entered.

Action
Confirm that you are using a valid key file.
Appendix G: Querying the Database Using the DB API

This appendix includes the following topics:

- The DB API Interface
- Components of the DB API

The DB API Interface

eHealth maintains information in an embedded Oracle database about the elements that it monitors. The DB API provides an interface that allows you to directly access this data by using standard SQL access techniques such as Oracle SQL*Plus or an ODBC driver interface. Object Database Connectivity (ODBC) is an open-standard API for accessing a database. By using ODBC statements in a program, you can access information from many different databases. You can then use this information, for example, with third-party reporting tools to create simple customized reports. The DB API is report-writer independent.

Important! You cannot use the DB API to access a Distributed eHealth Console.

For example, one connectivity model uses the SQL*Plus tool on the local eHealth system to connect to and query the eHealth database. You can also set up an ODBC connection to the eHealth system and access the eHealth Oracle service remotely; any standard method supported by Oracle is supported, including ODBC and JDBC.

Figure 2 shows this connectivity model for using the DB API.
To directly access eHealth® statistics data in the Oracle™ database, you can use the database application programming interface (DB API). To use this interface, you should have experience with the following technologies:

- Structured Query Language (SQL)
- Oracle relational databases
- Oracle SQL*Plus® utility
- Third-party reporting tools such as Crystal Reports

Components of the DB API

The DB API consists of a set of tables and views that provide coherent access directly to the database schema. The tables store and maintain the eHealth configuration information. The views are dynamically created for each type of element in the eHealth system. Using the DB API, you can do the following:

- **Obtain specific information from the database to use in another application or as a service to a customer.** For example, you may need to obtain the polled speed of an element so that you can update your billing system (if the billing rate is different for different speeds.) You may want to obtain information about a specific element or a set of elements such as the child elements for a given parent element or the endpoints of a link.

- **Determine the kind of statistical information that is valid for a particular element.** For example, you may want information about a particular statistic and would like to know if it is available from eHealth.
View statistical data for a particular element over a period of time.
For example, you may need to obtain the average availability of a system over a period of time but the information is currently not easily accessible. A view is a virtual table that allows you to access data so that it appears as though the data was from a single table (although the data may be in many tables).

Create Views Using the DB API Utility

By default, the DB API is automatically installed on an eHealth system and automatic updates of the views occur with the latest statistics data from the database. You must use the nhDbApi command to create views and maintain the DB API. The command has the following syntax:

```
nhDbApi [-h] [-rev] [-createViews | -deleteViews | -updateStatistics | -autoUpdate <Yes|No> ]
```

The following table describes the DB API command syntax.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Displays the command usage.</td>
</tr>
<tr>
<td>-rev</td>
<td>Displays the product version.</td>
</tr>
<tr>
<td>-createViews</td>
<td>Creates statistics views for each element type. Also enables automatic updates of the views with the latest statistics data from the database.</td>
</tr>
<tr>
<td>-deleteViews</td>
<td>Deletes statistics views for each element type.</td>
</tr>
<tr>
<td>-updateStatistics</td>
<td>Updates the statistics data from the database. Use this argument only if you disable automatic updates.</td>
</tr>
<tr>
<td>-autoUpdate &lt;Yes</td>
<td>No&gt;</td>
</tr>
</tbody>
</table>

You must have eHealth administrative-level account permissions to manage the views. To use the DB API, you must create the views that provide the database schema by entering the following:

```
nhDbApi -createViews
```

To generate views for all element types in the eHealth system, you must use the -createViews argument after you upgrade eHealth, install a patch release, add a certification release, run the nhConvertDb command, or add a custom variable to the eHealth system.
Components of the DB API

User Account Permissions

eHealth account privileges determine your access to eHealth and to the eHealth database. You can use an eHealth account that has read-only privileges to use SQL*Plus to connect to the database, use select statements, or create other queries to the database.

**Important!** You must not write to, insert, or update information in the eHealth database. Doing so may cause eHealth to become unusable.

To manage views, you **must** use an eHealth administrative-level account that has read and write privileges to the eHealth database. This account allows you to do the following with the DB API utility:

- Create views.
- Delete views.
- Update statistical information.
- Enable or disable automatic updates.

You can also use the nhManageUsers command to create a user with read-only privileges. For more information on creating users or managing account permissions by using the nhManageUsers command, see the eHealth Commands and Environment Variables Reference Guide. For more information about account privileges, see Chapter 6: Configuring eHealth User Account Permissions.

Modify Time Zones

The eHealth database stores information using Coordinated Universal Time (UTC) timestamps, which are time-zone independent. When queried, Oracle formats the timestamps into date and time values that are in the local time zone of the client running the SQL session.

You can use the ALTER SESSION statement in SQL to modify the time zone of a client session. To set the session to a particular time zone, use the following syntax:

```
ALTER SESSION SET TIME_ZONE = 'time_zone_region'
```

For example, to set the time zone for a client session to United States Central Time, enter the following:

```
ALTER SESSION SET TIME_ZONE = 'US/Central'
```

For a list of possible values for the `time_zone_region` variable, see your SQL documentation.
Daylight Saving Time

Oracle 9i provides the capability to return data based on the base time zone (standard time during the winter and Daylight Saving Time during the summer). It uses a comprehensive knowledgebase of time zone information, both current and historical, to determine the correct time zone. The DB API uses this feature to report data based on current Daylight Saving Time rules. Therefore, you do not need to modify data for Daylight Saving Time.

Converting Timestamps

The DB API has two SQL functions that convert UTC and Oracle date and time values. It uses these functions to automatically convert internal date and time values to a formatted date and time value (the formatted_sample_time variable). However, you also can also use these functions in queries.

NH_DBAPI.NH_NUM_TO_DATE Function

This function converts a date and time that is in UTC format to the corresponding Oracle date and time value. The date and time value is the time zone of the client that is running the SQL session.

This function has the following syntax:

NH_DBAPI.NH_NUM_TO_DATE(UTC_NUMBER)

For example, if you enter the following:

select NH_DBAPI.NH_NUM_TO_DATE(1036778399) from Dual

Important! Dual is a dummy table that does not contain any data. Oracle uses Dual to perform direct expression evaluation.

Oracle returns the following value:

NH_DBAPI.NH_NUM_TO

-------------
11-8-2002-12:59:59

NH_DBAPI.NH_DATE_TO_NUM Function

This function converts a date and time that is in Oracle date and time format to the corresponding UTC format. The date and time value is in the time zone of the client that is running the SQL session.

This function has the following syntax:

NH_DBAPI.NH_DATE_TO_NUM(OracleDateTimeValue)
In the following example, the TO_DATE Oracle function specifies the Oracle format. For example, if you enter the following:

```
select NH_DBAPI.NH_DATE_TO_NUM(TO_DATE('11/8/2002 12:59:59', MM/DD/YYYY HH24:MI:SS')) from Dual
```

Oracle returns the following value:

1036778399

**nh_elem_assoc Table**

The nh_elem_assoc table defines relationships between elements by relating their element_ids in the parent_id and element_id columns. The assoc_type column defines the type of relationship. The following table describes the columns in the nh_elem_assoc table.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>element_id</td>
<td>number</td>
<td>11</td>
<td>Represents the ID from the nh_element table.</td>
</tr>
<tr>
<td>machine_id</td>
<td>number</td>
<td>11</td>
<td>Represents the ID from the nh_element table.</td>
</tr>
<tr>
<td>parent_id</td>
<td>number</td>
<td>11</td>
<td>Represents the ID from the nh_element table.</td>
</tr>
<tr>
<td>assoc_type</td>
<td>number</td>
<td>11</td>
<td>Represents the ID from the nh_assoc_type table.</td>
</tr>
</tbody>
</table>

The following table lists the indexes for the nh_elem_assoc table.

<table>
<thead>
<tr>
<th>Index Values</th>
<th>Unique</th>
</tr>
</thead>
<tbody>
<tr>
<td>element_id, assoc_type</td>
<td>No</td>
</tr>
<tr>
<td>parent_id, element_id, assoc_type, machine_id</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**nh_assoc_type Table**

The nh_assoc_type table defines the relationship type used in the nh_elem_assoc table. The following table describes the columns in the nh_assoc_type table.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assoc_type</td>
<td>number</td>
<td>11</td>
<td>A unique ID</td>
</tr>
<tr>
<td>label</td>
<td>varchar2</td>
<td>20</td>
<td>Name of the association type, suitable for display in a user interface</td>
</tr>
</tbody>
</table>
The following table lists the values for assoc_type.

<table>
<thead>
<tr>
<th>assoc_type</th>
<th>label</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Parent</td>
</tr>
<tr>
<td>1</td>
<td>Response Source</td>
</tr>
<tr>
<td>2</td>
<td>Response Destination</td>
</tr>
<tr>
<td>3</td>
<td>Data Collector</td>
</tr>
<tr>
<td>4</td>
<td>Device</td>
</tr>
<tr>
<td>7</td>
<td>Side A</td>
</tr>
<tr>
<td>8</td>
<td>Side Z</td>
</tr>
<tr>
<td>9</td>
<td>Response Workgroup</td>
</tr>
<tr>
<td>10</td>
<td>Response Path Set</td>
</tr>
</tbody>
</table>

**NH_DBAPI_CATALOG Table**

The NH_DBAPI_CATALOG table maintains a catalog of the available element types, a description of each element, and the name of the view containing that element’s statistical information. You can use this table to determine the appropriate view to use for a particular element type. The following table describes the columns in the NH_DBAPI_CATALOG table.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE_ID</td>
<td>number</td>
<td>11</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>varchar2</td>
<td>30</td>
</tr>
<tr>
<td>VIEW_NAME</td>
<td>varchar2</td>
<td>64</td>
</tr>
</tbody>
</table>

The following table lists the default contents of the NH_DBAPI_CATALOG table. The DB API supports these element types in Release 5.6.

The contents of the NH_DPAPI_CATALOG table will change if you create custom element types or add new element types as part of a certification release.

<table>
<thead>
<tr>
<th>TYPE_ID</th>
<th>Description</th>
<th>VIEW_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>104007</td>
<td>Apache Application Service</td>
<td>NHV_104007_S</td>
</tr>
<tr>
<td>104010</td>
<td>Exchange Application Service</td>
<td>NHV_104010_S</td>
</tr>
<tr>
<td>104011</td>
<td>Internet Information Server (IIS) Application Service</td>
<td>NHV_104011_S</td>
</tr>
<tr>
<td>104013</td>
<td>MS SQL Application Service</td>
<td>NHV_104013_S</td>
</tr>
<tr>
<td>TYPE_ID</td>
<td>Description</td>
<td>View_Name</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>104014</td>
<td>Oracle Application Service</td>
<td>NHV_104014_S</td>
</tr>
<tr>
<td>104018</td>
<td>Switch Lite Backplane</td>
<td>NHV_104018_S</td>
</tr>
<tr>
<td>104019</td>
<td>Switch Plus Backplane</td>
<td>NHV_104019_S</td>
</tr>
<tr>
<td>104022</td>
<td>Generic Router/Switch CPU</td>
<td>NHV_104022_S</td>
</tr>
<tr>
<td>104023</td>
<td>Router/Switch CPU with Cache</td>
<td>NHV_104023_S</td>
</tr>
<tr>
<td>104024</td>
<td>Switch CPU</td>
<td>NHV_104024_S</td>
</tr>
<tr>
<td>104025</td>
<td>System CPU</td>
<td>NHV_104025_S</td>
</tr>
<tr>
<td>104026</td>
<td>Remote Access CPU</td>
<td>NHV_104026_S</td>
</tr>
<tr>
<td>104032</td>
<td>Frame Relay Permanent Virtual Circuit (PVC)</td>
<td>NHV_104032_S</td>
</tr>
<tr>
<td>104034</td>
<td>Generic Disk</td>
<td>NHV_104034_S</td>
</tr>
<tr>
<td>104035</td>
<td>BMC Disk</td>
<td>NHV_104035_S</td>
</tr>
<tr>
<td>104036</td>
<td>SystemEDGE Disk</td>
<td>NHV_104036_S</td>
</tr>
<tr>
<td>104039</td>
<td>Generic User Partition</td>
<td>NHV_104039_S</td>
</tr>
<tr>
<td>104040</td>
<td>BMC NT User Partition</td>
<td>NHV_104040_S</td>
</tr>
<tr>
<td>104041</td>
<td>BMC UNIX User Partition</td>
<td>NHV_104041_S</td>
</tr>
<tr>
<td>104042</td>
<td>SystemEDGE NT User Partition</td>
<td>NHV_104042_S</td>
</tr>
<tr>
<td>104043</td>
<td>SystemEDGE UNIX User Partition</td>
<td>NHV_104043_S</td>
</tr>
<tr>
<td>104045</td>
<td>Generic System Partition</td>
<td>NHV_104045_S</td>
</tr>
<tr>
<td>104046</td>
<td>BMC NT System Partition</td>
<td>NHV_104046_S</td>
</tr>
<tr>
<td>104047</td>
<td>BMC UNIX System Partition</td>
<td>NHV_104047_S</td>
</tr>
<tr>
<td>104048</td>
<td>SystemEDGE NT System Partition</td>
<td>NHV_104048_S</td>
</tr>
<tr>
<td>104049</td>
<td>SystemEDGE UNIX System Partition</td>
<td>NHV_104049_S</td>
</tr>
<tr>
<td>104052</td>
<td>Generic LAN Interface</td>
<td>NHV_104052_S</td>
</tr>
<tr>
<td>104053</td>
<td>Ethernet Interface</td>
<td>NHV_104053_S</td>
</tr>
<tr>
<td>104055</td>
<td>Token Ring Interface</td>
<td>NHV_104055_S</td>
</tr>
<tr>
<td>104060</td>
<td>Generic Modem</td>
<td>NHV_104060_S</td>
</tr>
<tr>
<td>104061</td>
<td>Integrated Services Digital Network (ISDN) Modem</td>
<td>NHV_104061_S</td>
</tr>
<tr>
<td>104063</td>
<td>Generic Modem Pool</td>
<td>NHV_104063_S</td>
</tr>
<tr>
<td>104068</td>
<td>NT Process</td>
<td>NHV_104068_S</td>
</tr>
<tr>
<td>TYPE_ID</td>
<td>Description</td>
<td>View_Name</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>104069</td>
<td>UNIX Process</td>
<td>NHV_104069_S</td>
</tr>
<tr>
<td>104072</td>
<td>NT Process Set</td>
<td>NHV_104072_S</td>
</tr>
<tr>
<td>104073</td>
<td>UNIX Process Set</td>
<td>NHV_104073_S</td>
</tr>
<tr>
<td>104075</td>
<td>Generic Application Service Process Set</td>
<td>NHV_104075_S</td>
</tr>
<tr>
<td>104077</td>
<td>Excluded NT Process Set</td>
<td>NHV_104077_S</td>
</tr>
<tr>
<td>104078</td>
<td>Excluded UNIX Process Set</td>
<td>NHV_104078_S</td>
</tr>
<tr>
<td>104082</td>
<td>Generic Response Path Set</td>
<td>NHV_104082_S</td>
</tr>
<tr>
<td>104084</td>
<td>Generic Remote Access Server (RAS)</td>
<td>NHV_104084_S</td>
</tr>
<tr>
<td>104093</td>
<td>Generic Response Path</td>
<td>NHV_104093_S</td>
</tr>
<tr>
<td>104094</td>
<td>Response Path with Jitter</td>
<td>NHV_104094_S</td>
</tr>
<tr>
<td>104095</td>
<td>Application Response Path</td>
<td>NHV_104095_S</td>
</tr>
<tr>
<td>104096</td>
<td>AR Response Path</td>
<td>NHV_104096_S</td>
</tr>
<tr>
<td>104097</td>
<td>Service Availability Response Path</td>
<td>NHV_104097_S</td>
</tr>
<tr>
<td>104099</td>
<td>Generic Router/Switch</td>
<td>NHV_104099_S</td>
</tr>
<tr>
<td>104100</td>
<td>Router Switch with CPU</td>
<td>NHV_104100_S</td>
</tr>
<tr>
<td>104102</td>
<td>Generic System</td>
<td>NHV_104102_S</td>
</tr>
<tr>
<td>104103</td>
<td>ManageWise System</td>
<td>NHV_104103_S</td>
</tr>
<tr>
<td>104104</td>
<td>Insight System</td>
<td>NHV_104104_S</td>
</tr>
<tr>
<td>104105</td>
<td>BMC NT System</td>
<td>NHV_104105_S</td>
</tr>
<tr>
<td>104106</td>
<td>BMC UNIX System</td>
<td>NHV_104106_S</td>
</tr>
<tr>
<td>104107</td>
<td>SystemEDGE NT System</td>
<td>NHV_104107_S</td>
</tr>
<tr>
<td>104108</td>
<td>SystemEDGE UNIX System</td>
<td>NHV_104108_S</td>
</tr>
<tr>
<td>104114</td>
<td>Generic WAN Interface</td>
<td>NHV_104114_S</td>
</tr>
<tr>
<td>104116</td>
<td>Asynchronous Transfer Mode (ATM) WAN Port</td>
<td>NHV_104116_S</td>
</tr>
<tr>
<td>104117</td>
<td>ATM WAN Path Side</td>
<td>NHV_104117_S</td>
</tr>
<tr>
<td>104118</td>
<td>ATM WAN Channel Side</td>
<td>NHV_104118_S</td>
</tr>
<tr>
<td>104120</td>
<td>Adaptive Rate Digital Subscriber Line (DSL)</td>
<td>NHV_104120_S</td>
</tr>
<tr>
<td>TYPE_ID</td>
<td>Description</td>
<td>View_Name</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>104121</td>
<td>Fixed Rate DSL</td>
<td>NHV_104121_S</td>
</tr>
<tr>
<td>104123</td>
<td>Frame Relay PVC Side</td>
<td>NHV_104123_S</td>
</tr>
<tr>
<td>104124</td>
<td>Visual Frame Relay PVC Side</td>
<td>NHV_104124_S</td>
</tr>
<tr>
<td>104125</td>
<td>Mobile Data Base Station (MDBS) WAN Interface</td>
<td>NHV_104125_S</td>
</tr>
<tr>
<td>104129</td>
<td>Alcatel Device Statistics</td>
<td>NHV_104129_S</td>
</tr>
<tr>
<td>104130</td>
<td>Alcatel Slot Statistics</td>
<td>NHV_104130_S</td>
</tr>
<tr>
<td>104131</td>
<td>RAS Digital Channel</td>
<td>NHV_104131_S</td>
</tr>
<tr>
<td>104132</td>
<td>Cisco AS5x00 Remote Access</td>
<td>NHV_104132_S</td>
</tr>
<tr>
<td>104133</td>
<td>Cisco RAS Channelized T1/E1</td>
<td>NHV_104133_S</td>
</tr>
<tr>
<td>104136</td>
<td>Nortel CVX Modem</td>
<td>NHV_104136_S</td>
</tr>
<tr>
<td>104137</td>
<td>Nortel CVX 1800 RAS</td>
<td>NHV_104137_S</td>
</tr>
<tr>
<td>104138</td>
<td>Nortel CSG Trunk</td>
<td>NHV_104138_S</td>
</tr>
<tr>
<td>104140</td>
<td>Quality of Service (QoS) Class of Service (CoS)</td>
<td>NHV_104140_S</td>
</tr>
<tr>
<td>104141</td>
<td>QoS CoS Contract</td>
<td>NHV_104141_S</td>
</tr>
<tr>
<td>104143</td>
<td>Cable LAN</td>
<td>NHV_104143_S</td>
</tr>
<tr>
<td>104144</td>
<td>Cable LAN Downstream Channel</td>
<td>NHV_104144_S</td>
</tr>
<tr>
<td>104145</td>
<td>Cable LAN Upstream Channel</td>
<td>NHV_104145_S</td>
</tr>
<tr>
<td>104146</td>
<td>Voice Gateway</td>
<td>NHV_104146_S</td>
</tr>
<tr>
<td>104147</td>
<td>Voice Digital Signal Zero (DS0)</td>
<td>NHV_104147_S</td>
</tr>
<tr>
<td>104148</td>
<td>Voice Peer-to-Peer Link</td>
<td>NHV_104148_S</td>
</tr>
<tr>
<td>104150</td>
<td>Wireless LAN</td>
<td>NHV_104150_S</td>
</tr>
<tr>
<td>104151</td>
<td>Generic Digital Signal Processing (DSP) Card</td>
<td>NHV_104151_S</td>
</tr>
<tr>
<td>104152</td>
<td>Voice Gateway CPU</td>
<td>NHV_104152_S</td>
</tr>
<tr>
<td>104153</td>
<td>Apache Application Service Process Set</td>
<td>NHV_104153_S</td>
</tr>
<tr>
<td>104154</td>
<td>Domain Name System (DNS) Application Service Process Set</td>
<td>NHV_104154_S</td>
</tr>
<tr>
<td>104155</td>
<td>eHealth Application Service Process Set</td>
<td>NHV_104155_S</td>
</tr>
<tr>
<td>TYPE_ID</td>
<td>Description</td>
<td>View_Name</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>104156</td>
<td>Exchange Application Service Process Set</td>
<td>NHV_104156_S</td>
</tr>
<tr>
<td>104157</td>
<td>IIS Application Service Process Set</td>
<td>NHV_104157_S</td>
</tr>
<tr>
<td>104158</td>
<td>Lotus Notes Application Service Process Set</td>
<td>NHV_104158_S</td>
</tr>
<tr>
<td>104159</td>
<td>MS SQL Server Application Service Process Set</td>
<td>NHV_104159_S</td>
</tr>
<tr>
<td>104160</td>
<td>Oracle Application Service Process Set</td>
<td>NHV_104160_S</td>
</tr>
<tr>
<td>104164</td>
<td>WAN Interface with Peak Statistics</td>
<td>NHV_104164_S</td>
</tr>
<tr>
<td>104165</td>
<td>ATM WAN Port with Peak Statistics</td>
<td>NHV_104165_S</td>
</tr>
<tr>
<td>104166</td>
<td>ATM Channel with Peak Statistics</td>
<td>NHV_104166_S</td>
</tr>
<tr>
<td>104167</td>
<td>Frame Relay Circuit with Peak Statistics</td>
<td>NHV_104167_S</td>
</tr>
<tr>
<td>104170</td>
<td>FireWall-1 Management Station Application Service</td>
<td>NHV_104170_S</td>
</tr>
<tr>
<td>104171</td>
<td>FireWall-1 Management Station Application Service Process Set</td>
<td>NHV_104171_S</td>
</tr>
<tr>
<td>104172</td>
<td>FireWall-1 Enforcement Point Application Service</td>
<td>NHV_104172_S</td>
</tr>
<tr>
<td>104173</td>
<td>FireWall-1 Enforcement Point Application Service Process Set</td>
<td>NHV_104173_S</td>
</tr>
<tr>
<td>104716</td>
<td>Network Services Sendmail UNIX Application Service</td>
<td>NHV_104716_S</td>
</tr>
<tr>
<td>104717</td>
<td>Network Services Sendmail UNIX Process Set</td>
<td>NHV_104717_S</td>
</tr>
<tr>
<td>104718</td>
<td>Network Services network information service (NIS) UNIX Application Service</td>
<td>NHV_104718_S</td>
</tr>
<tr>
<td>104719</td>
<td>Network Services NIS UNIX Process Set</td>
<td>NHV_104719_S</td>
</tr>
<tr>
<td>104720</td>
<td>Network Services line print (LP) Application Service</td>
<td>NHV_104720_S</td>
</tr>
<tr>
<td>104721</td>
<td>Network Services LP UNIX Process Set</td>
<td>NHV_104721_S</td>
</tr>
<tr>
<td>104722</td>
<td>Network Services DNS UNIX Application Service</td>
<td>NHV_104722_S</td>
</tr>
<tr>
<td>TYPE_ID</td>
<td>Description</td>
<td>View_Name</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>104723</td>
<td>Network Services DNS UNIX Process Set</td>
<td>NHV_104723_S</td>
</tr>
<tr>
<td>104724</td>
<td>Network Services Lightweight Directory Access Protocol (LDAP) UNIX Process Set</td>
<td>NHV_104724_S</td>
</tr>
<tr>
<td>104725</td>
<td>Network Services network file system (NFS) UNIX Process Set</td>
<td>NHV_104725_S</td>
</tr>
<tr>
<td>104727</td>
<td>Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Section</td>
<td>NHV_104727_S</td>
</tr>
<tr>
<td>104728</td>
<td>SONET/SDH Line</td>
<td>NHV_104728_S</td>
</tr>
<tr>
<td>104729</td>
<td>SONET/SDH Path</td>
<td>NHV_104729_S</td>
</tr>
<tr>
<td>104734</td>
<td>Network Services Active Directory NT Application Service</td>
<td>NHV_104734_S</td>
</tr>
<tr>
<td>104735</td>
<td>Network Services Active Directory NT Process Set</td>
<td>NHV_104735_S</td>
</tr>
<tr>
<td>104736</td>
<td>Network Services Dynamic Host Configuration Protocol (DHCP) NT Application Service</td>
<td>NHV_104736_S</td>
</tr>
<tr>
<td>104737</td>
<td>Network Services DHCP NT Process Set</td>
<td>NHV_104737_S</td>
</tr>
<tr>
<td>104738</td>
<td>Network Services DNS NT Application Service</td>
<td>NHV_104738_S</td>
</tr>
<tr>
<td>104739</td>
<td>Network Services DNS NT Process Set</td>
<td>NHV_104739_S</td>
</tr>
<tr>
<td>104740</td>
<td>Network Services Windows Internet Naming Service (WINS) NT Application Service</td>
<td>NHV_104740_S</td>
</tr>
<tr>
<td>104741</td>
<td>Network Services WINS NT Process Set</td>
<td>NHV_104741_S</td>
</tr>
<tr>
<td>104742</td>
<td>GTPS Tunnel Protocol (GTP) Tunnel</td>
<td>NHV_104742_S</td>
</tr>
<tr>
<td>104743</td>
<td>Fibre Channel</td>
<td>NHV_104743_S</td>
</tr>
<tr>
<td>104744</td>
<td>HTTP Proxy</td>
<td>NHV_104744_S</td>
</tr>
</tbody>
</table>

For a complete listing of supported elements, see NH_DBAPI CATALOG Table on page 307.
NH_ELEMENT Table

The NH_ELEMENT table maintains the identity of an eHealth element. It includes the fields that identify the element, such as name, alias, and ip_address. This table also maintains the TYPE_ID for a particular element so that the element links to the appropriate statistics view of the data. In addition, the table contains multiple attributes for an element that you can use for filtering.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>element_id</td>
<td>number</td>
<td>11</td>
<td>Specifies a unique ID for an element generated by eHealth.</td>
</tr>
<tr>
<td>machine_id</td>
<td>number</td>
<td>11</td>
<td>Specifies a unique machine ID for the eHealth system that “owns” the element.</td>
</tr>
<tr>
<td>name</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of the element.</td>
</tr>
<tr>
<td>name_lowercase</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of the element in lowercase letters.</td>
</tr>
<tr>
<td>alias</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the alias name of the &lt;Product Name&gt; element.</td>
</tr>
<tr>
<td>alias_lowercase</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the alias name of the &lt;Product Name&gt; element in lowercase letters.</td>
</tr>
<tr>
<td>ip_address</td>
<td>varchar2</td>
<td>21</td>
<td>Specifies the IP address of the element.</td>
</tr>
<tr>
<td>if_ip_address</td>
<td>char</td>
<td>15</td>
<td>Specifies the IP address of the interface. For elements that are MIB-II ifTable interfaces, this is the ipAdEntAddr value from the ipAddrEntry table matching the entry in the ifTable. In all other cases, it is the discovered IP address.</td>
</tr>
<tr>
<td>mtf_name</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the Management Information Base (MIB) translation file (MTF) name.</td>
</tr>
<tr>
<td>element_type</td>
<td>number</td>
<td>11</td>
<td>Specifies the element type ID.</td>
</tr>
<tr>
<td>latency_partner</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the IP address of a network device that is the latency partner of the element.</td>
</tr>
<tr>
<td>latency_source</td>
<td>number</td>
<td>11</td>
<td>For an element that is capable of alternate latency, specifies the type of latency to collect. This column applies only to devices polled using Simple Network Management Protocol (SNMP).</td>
</tr>
<tr>
<td>index1</td>
<td>number</td>
<td>11</td>
<td>Specifies a value that helps to create unique definitions for multiple elements on the same device.</td>
</tr>
<tr>
<td>index2</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies a value that helps to create unique definitions for multiple elements on the same device.</td>
</tr>
<tr>
<td>Column Name</td>
<td>Type</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index3</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies a value that helps to create unique definitions for multiple elements on the same device.</td>
</tr>
<tr>
<td>index4</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies a value that helps to create unique definitions for multiple elements on the same device.</td>
</tr>
<tr>
<td>speed</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the speed, or incoming speed of full-duplex elements, of an interface element in bits per second.</td>
</tr>
<tr>
<td>speed1</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the outgoing speed for full-duplex elements in bits per second.</td>
</tr>
<tr>
<td>device_speed</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the incoming speed of a device in bits per second.</td>
</tr>
<tr>
<td>device_speed2</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the outgoing speed of a device in bits per second.</td>
</tr>
<tr>
<td>response_limit</td>
<td>number</td>
<td>11</td>
<td>Specifies the element-specific limit on response time that appears in reports.</td>
</tr>
<tr>
<td>poll_rate</td>
<td>number</td>
<td>11</td>
<td>Specifies the rate at which polling occurs. The following are possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 – off</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 – normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 – slow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 – fast</td>
</tr>
<tr>
<td>poll_timeout</td>
<td>number</td>
<td>11</td>
<td>Overrides the NH_SNMP_TIMEOUT environment variable setting for the device on which the element resides.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NH_SNMP_TIMEOUT specifies the amount of time in microseconds that the poller waits for an SNMP response from an element before timing out and retrying the request.</td>
</tr>
<tr>
<td>poll_retries</td>
<td>number</td>
<td>11</td>
<td>Overrides the NH_SNMP_RETRIES environment variable setting for the device on which the element resides.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NH_SNMP_RETRIES specifies the maximum number of times that the poller sends an SNMP request to obtain data from an element during a poll.</td>
</tr>
<tr>
<td>community_string</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies a string that defines the specific MIB view for requesting variables.</td>
</tr>
<tr>
<td>Column Name</td>
<td>Type</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>read_community</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the SNMP community string for read access. This column is deprecated for Release 5.6 and above.</td>
</tr>
<tr>
<td>store_in_db</td>
<td>number</td>
<td>1</td>
<td>Specifies a boolean value that indicates whether to save the individual data for this element. This column is typically used for router interfaces, system interfaces, or system process elements. A value of 1 indicates that the database saves detailed data for the element.</td>
</tr>
<tr>
<td>remotely_polled</td>
<td>number</td>
<td>1</td>
<td>Indicates that the element is polled by a remote eHealth system. A value of 0 indicates the element is not remotely polled.</td>
</tr>
<tr>
<td>monitor_le</td>
<td>number</td>
<td>1</td>
<td>Specifies a boolean value that states whether eHealth should monitor this element using Live Exceptions. A value of 0 indicates that eHealth does not monitor the element.</td>
</tr>
<tr>
<td>full_duplex</td>
<td>number</td>
<td>1</td>
<td>Specifies a boolean value that specifies whether an element is full duplex. A value of 0 indicates that the element is not full duplex.</td>
</tr>
<tr>
<td>inc_in_lw_rpts</td>
<td>number</td>
<td>1</td>
<td>Represents an internal column used by eHealth.</td>
</tr>
<tr>
<td>hostname</td>
<td>varchar2</td>
<td>64</td>
<td>Indicates the hostname that uniquely identifies a device within the network on which the element resides.</td>
</tr>
<tr>
<td>sys_name</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the system name information obtained from the MIB.</td>
</tr>
<tr>
<td>sys_descr</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the system description information obtained from the MIB.</td>
</tr>
<tr>
<td>virtual_id</td>
<td>varchar2</td>
<td>32</td>
<td>Specifies a unique identifier for each logical element that exists on a single physical interface.</td>
</tr>
<tr>
<td>unique_dev_id</td>
<td>varchar2</td>
<td>128</td>
<td>Specifies a value that identifies the hardware such as a chassis ID or media access control (MAC) address of the device on which the element is being polled.</td>
</tr>
<tr>
<td>nms_key</td>
<td>varchar2</td>
<td>128</td>
<td>Specifies a key comprising several element attributes used to compare elements for uniqueness with the configuration.</td>
</tr>
</tbody>
</table>
Components of the DB API

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
</table>
| nms_state              | number    | 11     | Specifies whether the element exists on the network device and whether eHealth polls it. The following are possible values:  
<p>|                        |           |        | active – the element exists on the device and eHealth polls it.             |
|                        |           |        | deleted – the element has been deleted from the network management system (NMS) (or other configuration source) only. The element is not deleted from the eHealth database. |
| if_phys_address        | char      | 17     | Specifies the physical address of the interface.                            |
| device_hash_key        | varchar2  | 16     | Represents an internal column used by eHealth.                              |
| elem_timezone          | varchar2  | 20     | Specifies the time zone in which the element is located.                    |
| app_type               | number    | 11     | Specifies the application type for which this element collects data. The default is 0. |
| app_key                | varchar2  | 64     | Represents an internal column used by eHealth.                              |
| client_access          | varchar2  | 64     | Represents an internal column used by eHealth.                              |
| caption                | varchar2  | 64     | Represents an internal column used by eHealth.                              |
| user_string            | varchar2  | 256    | Specifies custom configuration data for the element.                        |
| import_module_name     | varchar2  | 10     | Specifies the name of the integration module that imports data for this element. This column currently applies only to the eHealth – Cisco CNS-PerfE integration module. The only valid value is cnspe. |
| import_nms_host        | varchar2  | 64     | Specifies the third-party NMS host that collects statistics for this element. This column currently applies only to the eHealth – Cisco CNS-PerfE integration module. eHealth ignores this column for any other element. |
| create_time            | number    | 11     | Specifies the UTC time when the element was created.                       |
| modify_time            | number    | 11     | Specifies the UTC time when the element was last modified.                 |</p>
<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>override_speed</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the incoming override speed of an interface element in bits per second.</td>
</tr>
<tr>
<td>override_speed1</td>
<td>number</td>
<td>38, 7</td>
<td>Specifies the outgoing override speed of an interface element in bits per second.</td>
</tr>
<tr>
<td>discover_mtf</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of the MTF that &lt;Product Name&gt; assigned when it discovered the element.</td>
</tr>
<tr>
<td>discover_community</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the community string used to discover the element.</td>
</tr>
<tr>
<td>sys_location</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the system location information. The default is an empty string (&quot; &quot;).</td>
</tr>
<tr>
<td>sys_contact</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the system contact information. The default is an empty string (&quot; &quot;).</td>
</tr>
<tr>
<td>if_desc</td>
<td>varchar2</td>
<td>128</td>
<td>Specifies the interface description. The default is an empty string (&quot; &quot;).</td>
</tr>
<tr>
<td>seg_name_mod_in_ui</td>
<td>number</td>
<td>1</td>
<td>Specifies whether a user modified the name of the element in the Poller Configuration dialog.</td>
</tr>
<tr>
<td>nms_name</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of the element at the NMS. The default value is an empty string (&quot; &quot;).</td>
</tr>
<tr>
<td>nms_source</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of the NMS source of this element.</td>
</tr>
<tr>
<td>enterprise_id</td>
<td>varchar2</td>
<td>32</td>
<td>Specifies the enterprise number that identifies the vendor of the SNMP agent running on the device to which the element belongs.</td>
</tr>
<tr>
<td>data_source_caps</td>
<td>varchar2</td>
<td>1024</td>
<td>For eHealth — Response elements, specifies the set of protocols that the polled device supports.</td>
</tr>
<tr>
<td>aggregate_avail</td>
<td>number</td>
<td>1</td>
<td>Specifies whether you want to include an application process in availability calculations for a process set.</td>
</tr>
<tr>
<td>args_required</td>
<td>number</td>
<td>1</td>
<td>Specifies whether you need to include arguments to uniquely identify a process.</td>
</tr>
<tr>
<td>process_args</td>
<td>varchar2</td>
<td>256</td>
<td>Specifies the arguments to include in a process definition to uniquely identify the process.</td>
</tr>
<tr>
<td>process_name</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies the name of an application process.</td>
</tr>
<tr>
<td>if_type</td>
<td>varchar2</td>
<td>32</td>
<td>Specifies the type for an interface element. The default is an empty string (&quot; &quot;).</td>
</tr>
</tbody>
</table>
Using Views for Each Element Type

You can use views to obtain statistical information for an element in the eHealth database. Each view has a variable number of columns of statistics data based on the type of element that you select. Each type of element has one view.

The view that you choose must match the type of element on which you are reporting. If it does not match, the output data from the query contains incorrect information.

Each view includes the system time as defined by the time zone of the client running the SQL*Plus session. The view definition converts the date and time format from UTC to the Oracle date and time format.

To use views for an element

1. Determine the View_Name of the element. View_names are based on the type of element. You can determine the View_Name by using the information in NH_DBAPI_CATALOG Table on page 307 or you can run a SQL command. The following is an example of a SQL command for an element named MIS-SH-Cpu-1:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>possible_latency_srcs</td>
<td>varchar2</td>
<td>64</td>
<td>Specifies whether the element supports alternate latency. This field applies only to devices that are polled using SNMP.</td>
</tr>
<tr>
<td>protocol_cfg</td>
<td>varchar2</td>
<td>2048</td>
<td>For eHealth — Response elements, specifies the protocol used to measure response time and associated variables between the two endpoints of a response path.</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>11</td>
<td>Defines the trap destination’s port number. The default is 162 for most trap destinations.</td>
</tr>
<tr>
<td>polling_enabled</td>
<td>number</td>
<td>1</td>
<td>Indicates whether &lt;Product Name&gt; polls the element: 1 (the default) enables importing data for the element. 0 disables importing.</td>
</tr>
<tr>
<td>polling_region</td>
<td>varchar2</td>
<td>64</td>
<td>Enables distribution of requests to groups of devices across slow links.</td>
</tr>
</tbody>
</table>

Column Name Type Length Description
select name, elementId, elementType from
nh_element where name = 'MIS-SH-Cpu-1';

The command outputs the following:

<table>
<thead>
<tr>
<th>NAME</th>
<th>ELEMENTID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIS-SH-Cpu-1</td>
<td>1000014</td>
</tr>
<tr>
<td>104025</td>
<td>104025</td>
</tr>
</tbody>
</table>

View_Names consist of an NHV_ prefix and a _S suffix to the elementType. In the example shown above, the View_Name is NHV_104025_S.

2. Determine the supported variables for the element.
3. Run SQL commands to obtain the statistical information.

**Determine the Supported Variables for an Element**

To display the variables that are available for a specific type of element, use the describe command with the View_Name in SQL*Plus. For example, to determine the information available for a system CPU element, enter the following:

```sql
describe NHV_104025_S
```

The command outputs the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Null?</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELEMENTID</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>FORMATTED_SAMPLE_TIME</td>
<td></td>
<td>DATE</td>
</tr>
<tr>
<td>SAMPLE_TIME</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>DELTATIME</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>TOTALTIME</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>GOODPOLLS</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>MISSEDPOLLS</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>BADPOLLS</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>REBOOTS</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>CPUUTILIZATION</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>AVAILABILITY</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>REACHABILITY</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>LATENCY</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>CPUIDLEUTILIZATION</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>CPUUSERUTILIZATION</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>CPUSYSTEMUTILIZATION</td>
<td></td>
<td>NUMBER</td>
</tr>
<tr>
<td>CPUWAITUTILIZATION</td>
<td></td>
<td>NUMBER</td>
</tr>
</tbody>
</table>
Error Conditions

Errors may occur in the following areas:

- The execution of the scripts that create the views
- The execution of SQL code against the created views
- The amount of as-polled data and number of statistics tables that can be supported

The following sections detail these error conditions and describe how to resolve them.

Errors in Script Execution

The following sections describe the errors you can receive when the SQL script executes.

Triggers Fail When Updating Statistics

A trigger is a set of SQL statements that automatically execute an action when a specific event occurs. The following two error conditions can occur due to problems with triggers:

- An error appears in the console window stating that a failure occurred when inserting or deleting statistics data in the database because a trigger failed. To resolve this error, log on to the database and disable the trigger. This problem may have occurred because too much raw data was saved in the database.
- A message appears in the console window indicating that the trigger was unable to execute successfully. The database failed to recreate a view when Oracle inserted or deleted a table from the database. To resolve this error, run the nhDbApi command using the -updateStatistics argument to update the statistical data from the database.

Failure When Creating One or More Views

In some cases, the database does not create one or more views due to errors originally made by a user creating a custom variable. A warning appears and identifies the view that failed to create. To resolve this error, review the custom variable information. For more information, see the eHealth Customizing Variables Administration Guide.
Errors in SQL Code

When SQL code executes, the database can fail to return any rows of data or can return bad data. Poorly formed SQL queries can also return an error with an Oracle error message indicating the cause of the error. To verify the quality of the data, use the nhExportData command to output comparable results. For more information about this command, see the eHealth Data Integration Guide.

Errors in Amount of As-Polled Data and Number of Statistics Tables that Can Be Supported

The default statistics rollup table is two days of as-polled data, six weeks of hourly data, and 70 weeks of weekly data. If you modify the rollup schedule to maintain large amounts of raw data, there is a possibility that you may exceed the Oracle memory limit. The maximum amount of supported as-polled data is 30 days, and the maximum number of statistics tables cannot exceed 832. It is unlikely that you will encounter such an error situation unless you regularly maintain excessive amounts of raw data, for example, 12 months' worth.

How to Use Performance Analysis Tools for SQL Queries

The DB API provides direct access to data in the Oracle database. You can use any tracing and performance analysis tools to determine the performance of SQL queries. To determine the performance of a particular query, enable tracing for the SQL session that you want to analyze.

Troubleshoot Queries

To troubleshoot problems with DB API queries, you must first analyze the validity of your query. You can accomplish this by verifying that your query is working in SQL*Plus.

To verify that the queried data exists in the database

1. Start a SQL*Plus session by logging in as a read-only user.
2. Cut and paste the query into the SQL*Plus window.
3. Press Enter. Review the output from the query to determine if the data is valid.

If the data appears valid, the DB API is functioning appropriately, so the problem must exist in the reporting tool. Contact Professional Services for fee-based assistance to build customized reports using available third-party reporting tools.
4. If the output appears to be invalid, contact Technical Support and provide the following:
   - A text file that contains a copy of your query.
   - A text file that contains a copy of the data output from the query.
   - A detailed explanation of why the data appears to be invalid.

   In addition, they may require a copy of your database.

   **Important!** Technical Support is *not* responsible for creating your custom SQL queries or for troubleshooting problems encountered when importing to or using any third-party reporting tools with the DB API.

**Examples of Using the DB API**

This section provides examples of how to use the DB API utility.

**Export Data to an External File System**

Using the DB API, you can obtain data that is comparable to the output from the `nhExportData` command. The `nhExportData` command outputs information to a proprietary formatted datafile that you can use as input to another database or to create a flat comma-separated value (CSV) file.

The following example shows the output of the `nhExportData` command, which was used to obtain output for a system CPU element named SINK-SH-Cpu-1:

```plaintext
IR,2,D:\work\tmp\cpu.txt,0,06/03/2002,10:30:23,<UndefinedDbName>
FT,DataExport,string,string,floatNoExp,floatNoExp,string,integer,integer,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,floatNoExp,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,
``
To use the DB API to obtain this data

1. Create the views by running the nhDbApi command with the -createviews argument.

2. Open the Oracle SQL*Plus tool in a command window and obtain the elementId and elementType for the element by entering the following commands:

   sqlplus ehuser/ehuser
   SPOOL sink_cpu_data.out
   select name, elementId, elementType from nh_element where name = 'SINK-SH-Cpu-1';

The commands output the following:

<table>
<thead>
<tr>
<th>NAME</th>
<th>ELEMENTID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SINK-SH-Cpu-1</td>
<td>1000014</td>
</tr>
</tbody>
</table>

From this output, you can determine the elementId; and from the elementType you can determine the View_Name. Using the View_Name, run a query to determine the possible statistical information.

3. Using this information, specify the following export query:

   select e.name, s.name, s.elementId, s.formatted_sample_time, s.deltaTime, s.cpuUserUtilization, s.cpuSystemUtilization, s.cpuWaitUtilization, s.cpuIdleUtilization, s.goodPolls from NHV_104025_S s, nh_element e where s.elementId = 1000014 and e.elementId = s.elementId and s.formatted_sample_time >= TO_DATE('20-5-2002 9:59:59', 'DD-MM-YYYY HH24:MI:SS') and s.formatted_sample_time < TO_DATE('20-5-2002 10:59:59', 'DD-MM-YYYY HH24:MI:SS') AND s.deltaTime <> 0;
The following is a reformatted sample output from this query:

NAME, ELEMENTID, FORMATTED SAMPLE TIME, DELTATIME, CPUUSERUTILIZATION, CPUSYSTEMUTILIZATION, CPUWAITUTILIZATION, CPUIDLEUTILIZATION, GOODPOLLS, MISSEDPOLLS, BADPOLLS, REBOOTS, CPUUTILIZATION, LATENCY

SINK-SH-Cpu-1,1000014,5/30/2002 10:02:48 AM,303,0,1,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:07:48 AM,300,0,0,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:12:52 AM,304,0,0,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:17:52 AM,300,0,1,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:22:51 AM,299,0,1,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:27:51 AM,300,0,0,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:32:53 AM,302,0,0,0,100,100,0,0,0,0,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:37:53 AM,300,1,1,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:42:52 AM,299,0,1,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:47:52 AM,300,0,0,0,99,100,0,0,0,1,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:52:52 AM,300,2,3,0,95,100,0,0,0,5,1
SINK-SH-Cpu-1,1000014,5/30/2002 10:57:53 AM,301,6,9,0,86,100,0,0,0,14,1

Reachability and Availability

In the previous example, the export query provided statistics data for a system CPU element, excluding information about reachability and availability. To obtain information on reachability and availability, remove the following text from the export query:

s.deltaTime <> 0

As a result, the export query for reachability and availability information would be the following:

select e.name, s.name, s.elementId, s.formatted sample time, s.deltaTime, s.reachabilty, s.availabilty from NHV 104025 S s, nh_element e where s.elementId = 1000014 and e.elementId=s.elementId and s.formatted sample time >= TO_DATE('20-5-2002 9:59:59', 'DD-MM-YYYY HH24:MI:SS') and s.formatted sample time < TO_DATE('20-5-2002 10:59:59', 'DD-MM-YYYY HH24:MI:SS');

EXIT

The following is the sample output from this query:

NAME, ELEMENTID, FORMATTED SAMPLE TIME, DELTATIME, REACHABILITY, AVAILABILITY

SINK-SH-Cpu-1,1000014,5/30/2002 10:02:48 AM,303,100,100
SINK-SH-Cpu-1,1000014,5/30/2002 10:07:48 AM,300,100,100
SINK-SH-Cpu-1,1000014,5/30/2002 10:12:52 AM,304,100,100
SINK-SH-Cpu-1,1000014,5/30/2002 10:17:52 AM,300,100,100
SINK-SH-Cpu-1,1000014,5/30/2002 10:22:51 AM,299,100,100
Use a Third-Party Report-Writer Tool to Prepare Custom Reports

You can use the DB API to provide a consistent SQL interface to third-party reporting tools by using ODBC or JDBC drivers. Java Database Connectivity (JDBC) is an API specification for connecting programs written in Java to the data in databases. The third-party reporting tool can then create reports by querying the database using standard SQL queries.

To set up a Windows-based report-writer tool to access the DB API and the eHealth database

1. Use the nhConfigDbNet command to configure the SQL*net software on the eHealth system. For instructions, see the eHealth Commands and Environment Variables Reference Guide.
2. Obtain and install the Oracle client software on the report-writer client system (customer-furnished; not supplied by Concord).
3. Configure a SQL*Net client connection using the connection string specified in Step 1.
4. Create an ODBC driver.
5. Use this driver to connect to the eHealth database through Microsoft Excel, Crystal Reports, or any other report-writer tool.

Create an ODBC Driver

You can use an ODBC connection to access data in the eHealth database.

To create a new ODBC connection

1. Log on to the system using an eHealth administrative-level account.
2. Click Start, Settings, Control Panel. The Control Panel appears.
3. Double-click the Data Sources (ODBC) icon in the Administrative Tools folder of the Control Panel. The ODBC Data Source Administrator dialog appears.
4. Select the System DSN tab and click Add. The Create New Data Source dialog appears.
5. Select Oracle in OraHome92 from the list of ODBC drivers and click Finish. The Oracle ODBC Driver Configuration window appears.
Components of the DB API

6. Configure the ODBC driver by completing the fields as follows:
   a. Specify a connection name in the Data Source Name field.
   b. (Optional) Specify a description of the data source.
   c. Select the eHealth service from the TNS Service Name list.
   d. Specify the eHealth user account name in the User ID field.
7. Specify the server for the ODBC connection in the Server field, and click Next.
8. Test the ODBC connection by clicking Test Connection.
9. Click OK.

Create Reports using Microsoft Excel

You can use Microsoft Excel to create simple customized reports.

To create a report

1. Create the views by running the nhDbApi command with the -createviews argument.
2. Create an ODBC driver as described in the previous section.
3. Open Excel by selecting Start, Programs, Microsoft Excel.
   1. Select Data, Get External Data, New Database Query. The Choose Data Source dialog appears.
4. Select the Oracle ODBC connection and click OK. The ODBC Login dialog appears.
5. Do the following:
   a. Specify your eHealth user name in the User Name field.
   b. Specify the eHealth password in the Password field and click OK. The Microsoft Query window appears.
6. Select the View_Name that matches the element type and click Next. For example, select NHV_10425_S for a system CPU.
7. Specify whether you want to place the information in a new worksheet or an existing worksheet, and then click OK.

The data from which you can create a report appears in the worksheet.

Single Element Trend Reports

A third-party report-writer tool can generate a single element Trend report for any of the eHealth statistics variables available for that element. To obtain the information, the tool uses a SQL query that queries the database using the view based on the element type. The query returns sample data based on real time.

The following is an eHealth Trend report for a single element (CPU) with multiple variables.
You can also create this graph using Crystal Reports (a report-writer tool) using the following SQL query passed through an ODBC connection to the eHealth database:

```sql
select e.name, s.* from NHV_104025_S s, nh_element e
where s.elementId = 1000014 and e.elementId = s.elementId and
s.sampleTime >= TO_DATE('20-5-2002 9:59:59', 'DD-MM-YYYY HH24:MI:SS')
and s.sampleTime < TO_DATE('20-5-2002 10:59:59', 'DD-MM-YYYY HH24:MI:SS') and DELTATIME <> 0;
```

**Figure 4** shows the result of creating a Crystal report using the above query.
Components of the DB API

Figure 4 Crystal Trend Report
Appendix H: Database Layout File

This appendix includes the following topics:

- eHealth Database Layout Design
- eHealth Basic Database Schema
- Use an LCF during Installation to Size Your Database

eHealth Database Layout Design

As an alternative to the eHealth database creation process, you can create an eHealth database Layout Configuration File (LCF). This feature enables you to specifically place the various files of your database. You can use an LCF when you initially create the database during eHealth installation and after you install the product.

When you install eHealth on a new system (in which you have not previously installed eHealth), the installation program asks you to specify the locations in which you want to install the software and the database. It also asks you to choose the type of system that you would like to install. Once you provide that information, you must specify the database sizing method. The database sizing method is the process that eHealth follows to obtain information about your eHealth environment and to create a resulting database.

The installation process provides you with three options to size your database:

- Typical – Instructs the installation process to apply the eHealth database default settings to size and lay out your eHealth database based on the number of elements that you intend to poll and the amount of as-polled data that you intend to retain in your database.
- Detailed – Allows you to use a system sizing file (SSF) to obtain the eHealth database configuration settings. You can create an SSF using the eHealth 5.6 System Sizing Tool.
- Custom – Allows you to use an LCF to specify your database layout.

If you choose the Typical or Detailed option, you can specify a maximum of nine directories to use for the database, and the installation process automatically distributes your datafiles across those directories. If you prefer to specify the exact locations for the database tablespaces and datafiles, you must choose Custom as well as perform other steps described in the following sections.
The basic eHealth 5.6 database schema contains approximately 90 tables stored in the seven tablespaces listed in the following table. Over time, the number of database tables grows as eHealth creates new tables based on polling intervals and rollup activity.

**Important!** In this document the symbol K represents kilobytes, the symbol M represents megabytes, and the symbol G represents gigabytes.

<table>
<thead>
<tr>
<th>Tablespace Name</th>
<th>Contents or Usage</th>
<th>Sizing Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Objects that do not have a storage clause, and various system operations (Oracle’s default tablespace).</td>
<td>Approximately 200 to 300 M, regardless of the setting of the CfgDbModelSize configuration variable.</td>
</tr>
<tr>
<td>NH_ROLLBACK</td>
<td>All rollback segments.</td>
<td>Varies from 244 to 1000 M, depending on the setting of the CfgDbModelSize configuration variable.</td>
</tr>
<tr>
<td>NH_TEMP</td>
<td>Temporary tablespace for grouping and sorting operations during queries and reports.</td>
<td>Varies from 500 M to 2 G, depending on the setting of the CfgDbModelSize configuration variable.</td>
</tr>
<tr>
<td>NH_USERS</td>
<td>Poller configuration, and all other statically named tables that are not created during polling or rollups.</td>
<td>Varies from 4 M and greater, depending on the setting of the CfgNumElements and CfgNumDaysRaw configuration variables, and many others. For Traffic Accountant systems, this tablespace remains approximately 4 M.</td>
</tr>
<tr>
<td>NH_INDEX</td>
<td>All indexes, across all eHealth tables. For optimum performance, NH_INDEX should not be located on the same disk with NH_USERS, NH_DATA01, or NH_DATA02.</td>
<td>Varies from 4 M and greater, depending on the setting of the CfgNumElements and CfgNumDaysRaw configuration variables, and many others. This tablespace is used for standard eHealth and Traffic Accountant eHealth systems.</td>
</tr>
<tr>
<td>NH_DATA01</td>
<td>NH_DLG% - Raw Traffic Accountant data and all rollup data</td>
<td>Varies from 4 M and greater. This tablespace is quite large on all systems except Distributed eHealth Consoles (front-ends) which do not poll and do not have Traffic Accountant installed.</td>
</tr>
<tr>
<td></td>
<td>NH_STATS% - Raw statistics data and all rollup data</td>
<td></td>
</tr>
</tbody>
</table>
| NH_DATA02       | NH_BSLN% - Baselines | Varies from 4 M and greater. For eHealth Traffic Accountant and Distributed eHealth Consoles (front-ends) this tablespace remains approximately 4 M. | NH_DAILY_EXCEPTIONS%  
|                 | NH_DAILY_HEALTH%  
|                 | NH_DAILY_SYMBOL%  
|                 | NH_HOURLY_HEALTH%  
|                 | NH_HOURLY_VOLUME% | |
How to Use Your Disk Space More Efficiently

As an alternative to allowing eHealth to create your database for you automatically, you can use an LCF to specify exactly where eHealth should place each datafile. This enables you to use your disk space more efficiently and generate optimum performance for your eHealth system.

To customize your database, you can use one of the following three methods:

- **Use an LCF during installation to size your database.** For new installations and migrations, you can create an LCF before you install eHealth (or after starting the installation) to lay out your database as described in the next section, “Use an LCF during Installation to Size Your Database.” (eHealth 5.5 systems already have an Oracle database. If you want to resize it, recreate the database after upgrading to eHealth 5.6 as described in section on page 333.)

- **Extend your database to add more disk space, and then generate a new LCF based on the updated configuration.** After you install eHealth 5.6, you can use the nhManageDbSpace command to add datafiles to your eHealth tablespaces or move datafiles from one location to another. You can generate a new LCF from the existing database to record the changes. This method is described in section on page 332.

- **Recreate your database based on an LCF.** You can create an LCF after you install eHealth 5.6, and then run the nhCreateDb command using the `-i pathname` argument to create a new database based on the LCF. This method is described in section on page 333.

---

Use an LCF during Installation to Size Your Database

For new installations and migrations, the procedure for creating an LCF and using it during the installation to size your database is slightly different.

**To create an LCF and use it during new installations and migrations**

Run the eHealth 6.1 System Sizing Tool on any Windows 2000 system that has Internet Explorer 6.0. Even if you have eHealth CDs for UNIX, you can place the eHealth CD in a Windows 2000 CD-ROM drive and run the sizing tool.

1. Within the root directory of your eHealth software CD, locate the eHealth 5.6 System Sizing Tool (New_Install.xls).
2. Open the Excel file.
   - Important! For system requirements to run the tool, see the eHealth_61_System_Sizing_Tool.xls file located on the CD.
3. Respond to the sizing tool prompts.
4. Examine the report on the Summary tab to determine your disk space needs.
   - You can print this report to save for future use.
5. Record each tablespace size, and the Redo and Archive logs.
Use an LCF during Installation to Size Your Database

6. Create an LCF file by doing one of the following:
   - If you have not previously installed eHealth 6.1 on the target system, create a new file named `fileName`.lcf and store it in a secure place.
   - If you have already installed eHealth on the target system, create a copy of the LCF that the eHealth installation program produced automatically and placed in the `eHealth/oracle/database` directory. It is named `hostname_SID`.lcf, where `hostname` is the name of your system and `SID` is the name of your eHealth database (the value of the ORACLE_SID environment variable). Rename the copy as `fileName`.lcf and place the file in a secure place.

7. Compose the LCF by following the instructions provided in section on page 334. Follow the format shown in the sample LCFs provided in section on page 338.

8. After you finish specifying the location of your tablespaces and datafiles, save the file.

9. Do one of the following:
   - For new installations, run the eHealth installation program and respond to the prompts. When the program asks you to specify the database sizing method, select Custom and specify the pathname of your custom LCF.
   - For migrations, you must start the installation program by using the `-useLcf` argument and specifying the full pathname of the LCF.

10. Proceed with the remainder of the installation. The installation program creates the eHealth database based on the LCF specifications.

Extend Your Database to Add More Disk Space

To improve database performance after installing eHealth, you can use the `nhManageDbSpace` command to add datafiles to an eHealth tablespace, move datafiles from one location to another, and then generate a new LCF to create a record of the database layout. If you do not specify a name for the LCF in the command syntax, eHealth places the `hostname_SID`.lcf file in the `eHealth/oracle/database` directory.

**To extend your database and create a new LCF as a record**

1. Move a datafile from one location to another by entering the following at the command line:

   ```
   nhManageDbSpace -move -datafile datafileName -newPath directory
   ```

   where `datafileName` is the name of the datafile that you need to move, and `directory` is the location where you want to move the datafile.

   - If necessary, repeat Step 1 to move another datafile.

   - Add a datafile to a tablespace by entering the following:

   ```
   nhManageDbSpace -add -newPath directory -tablespace tablespace -size fileSize
   ```
Use an LCF during Installation to Size Your Database

where directory is the location of the new datafile, tablespace is the name of the tablespace to which you want to add the datafile, and fileSize is the initial size of the new datafile in megabytes.

For example, to add a datafile of 100 M to e:/oradata/SID/NH_INDEXxx.dbf, enter the following:

```
nhManageDbSpace -add -newPath e:/ -tablespace NH_INDEXxx -size 100M
```

SID is the name of your eHealth database (the value of the ORACLE_SID environment variable).

2. If necessary, repeat Step n to add more datafiles.

3. Create a new LCF based on the information in the database by entering the following:

```
nhManageDbSpace -createLCF
```

The command creates an LCF based on the current eHealth database and saves it as eHealth/oracle/database/hostname_SID.lcf, overwriting any existing LCF.

For detailed instructions on using the nhManageDbSpace command, see the eHealth Commands and Environment Variables Reference Guide. For more information on managing your eHealth database, see Chapter 7: Database Management.

Recreate Your Database Based on an LCF

After you install eHealth 5.6, you may decide that you want more control over where eHealth places the database datafiles. You can use the nhCreateDb command to recreate your database based on an LCF.

To recreate an eHealth database based on an LCF

1. Use the eHealth 5.6 System Sizing Tool to size your eHealth system and determine your disk space needs.

2. Create a copy of the LCF that the eHealth installation program produced automatically and placed in the eHealth/oracle/database directory. It is named hostname_SID.lcf, where hostname is the name of your system and SID is the name of your eHealth database. Rename the copy as fileName.lcf and place the file in a secure place.

3. Modify the LCF for your new database following the instructions provided in section on page 334. Follow the format shown in the sample LCFs provided in section on page 338.

4. After you finish specifying the location of your tablespaces and datafiles, save the file.

5. Save your database by performing a platform-independent Oracle save. Enter the following at the command line:

```
nhSaveDb -ascii -p pathname
```
Use an LCF during Installation to Size Your Database

where \texttt{pathname} must be a directory outside the database area that is large enough to hold a copy of the database.

Although the command argument is \texttt{-ascii}, eHealth creates a platform-independent Oracle save. It does \textit{not} create an ASCII database. If you do not specify \texttt{-ascii}, eHealth creates an Oracle Recovery Manager (RMAN) save, which you can only load back into the same system from which it came. Do \textit{not} perform a binary save. Binary saves return the existing layout; and when you load them, eHealth recreates your existing database layout.

6. Destroy your database by entering the following:

\texttt{nhDestroyDb}

7. Create a new database by entering the following:

\texttt{nhCreateDb -i \texttt{pathname}}

where \texttt{pathname} is the full pathname of the LCF. This command does not run interactively; it immediately begins to create the database using the parameters specified in the LCF. For example, the following command creates an eHealth database using an LCF named \texttt{madison.lcf} that resides in the \texttt{C:\temp} directory:

\texttt{nhCreateDb -i C:/temp/madison.lcf}

For detailed instructions for using the \texttt{nhCreateDb} command, see the \textit{eHealth Commands and Environment Variables Reference Guide}. For more information on managing your eHealth database, see \textit{Chapter 7: Database Management}.

8. Load data from the platform-independent Oracle save into the new database by entering the following:

\texttt{nhLoadDb -p \texttt{pathname}}

where \texttt{pathname} is the location in which you saved the database in Step 5.

\textbf{The Contents of the LCF File}

The LCF is composed of three types of information:

- **Configuration Variables** – Attributes that describe your eHealth system and database.

- **Software Locations** – Directories in which the eHealth and Oracle software are located. If you have an existing installation, these directories must be the same as those specified during the installation. If you have not yet installed eHealth, these values will override whatever you specify in the installation.

- **Database File Layout** – Directories or tablespaces in which eHealth should store the datafiles, the size of each directory, and the locations of the datafiles on a local disk partition.
Syntax Guidelines

Within each line of the LCF, you can use the following:

- Spaces, tabs, and newlines to format the values
- Full-line comments and end-of-line comments (denoted by the use of the # symbol)
- Spaces within pathnames (if the pathname is enclosed in double quotation marks)
- Slashes in either direction (backward or forward)
- Explicit versioning in the file
- The token \{SID\} that represents the eHealth database name

If you are using a localized version of eHealth, do not specify accented characters in the pathnames and directory names.

Specify the Configuration Variables

You can specify configuration variables such as CfgHostname and CfgDbModelSize to define the attributes that describe your eHealth system and database.

To provide this information, use the following syntax:

```
CfgSettingName = settingValue
```

where `settingName` is the specific configuration variable and `settingValue` is the value of the variable. For example, `CfgDbName` specifies the name of the database. The following table lists the configuration variables that you can define in an LCF, indicates whether they are required or optional, and defines their purpose and required values.

<table>
<thead>
<tr>
<th>Configuration Variable Name</th>
<th>Required</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CfgHostname</td>
<td>Yes</td>
<td>Specifies the hostname of the eHealth system. The value must match the setting of the NH_HOSTNAME environment variable, if eHealth is already installed.</td>
</tr>
</tbody>
</table>
| CfgDbModelSize              | Yes      | Specifies the size of the database. The following are valid values:  
  - small (for systems that poll less than 3000 elements every 5 minutes)  
  - medium (for systems that poll 3000 to 10,000 elements)  
  - large (for systems that poll 10,000 to 25,000 elements)  
  - xlarge (for systems that poll over 25,000 elements) |
Use an LCF during Installation to Size Your Database

<table>
<thead>
<tr>
<th>Configuration Variable Name</th>
<th>Required</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CfgSID</td>
<td>Yes</td>
<td>Specifies the name of the eHealth database, which is also the Oracle SID. The value must match the setting of the NH_ORACLE_SID environment variable, which has a default value of eHealth, if eHealth is already installed.</td>
</tr>
<tr>
<td>CfgRedoLogSize</td>
<td>Yes</td>
<td>Specifies the size of the database redo log.</td>
</tr>
<tr>
<td>CfgNH_USER</td>
<td>Yes</td>
<td>Specifies the name of the eHealth user. The value must match the setting of the NH_USER environment variable, if eHealth is already installed.</td>
</tr>
<tr>
<td>CfgOverrideSpaceCheck</td>
<td>No</td>
<td>Overrides disk space checking (designed for use with sites that use disk compression).</td>
</tr>
<tr>
<td>CfgPercentCapacityReserveDb</td>
<td>No</td>
<td>Specifies the percentage of growth that should be reserved for database files. A value of 1% creates a disk reserve of 1%; whereas a value of 100% creates a disk reserve of 100% (this would double the database disk space requirement for eHealth). By default, eHealth creates a 10% reserve for database files.</td>
</tr>
<tr>
<td>CfgPercentCapacityReserveWeb</td>
<td>No</td>
<td>Specifies the percentage of disk drive space for the eHealth/web/output directory that should be reserved for eHealth growth or non-eHealth use. This directory contains reports scheduled for Web output and reports run on demand by Web users. A value of 1% would create a disk reserve of 1% of the estimated size of the web/output directory. A value of 100% would create a disk reserve of 100%, double the size of the Web output directory. By default, eHealth creates a 20% reserve.</td>
</tr>
</tbody>
</table>

If you need to define additional configuration variables within the LCF, see your system sizing file and contact Technical Support for guidance.

The following is an example of Configuration Variable information specified in an LCF:

```plaintext
CfgSystemType = BackEnd
CfgSID = JOE101
CfgNumElements = 1
CfgHostname = system1
CfgDbModelSize = medium
CfgDaysRaw = 1
CfgNH_USER = nhuser
CfgRedoLogSize = 62M
```
Provide the Software Locations

In addition to listing the configuration variables, you must provide the input for the layout, specifying the directories into which the installation program must install software products (for example, eHealth and Oracle).

If you have already installed eHealth, the following pathnames are required:

- **NH_HOME** – The pathname must match the setting of the NH_HOME environment variable, which is the eHealth installation directory.
- **NH_ORACLE_HOME** – The pathname must match the setting of the NH_ORACLE_HOME environment variable, which is the Oracle software installation directory.

If you are using an LCF to recreate your database, these environment variables do not exist yet.

The following is an example:

```
NH_HOME -/export/system1/mar30_rlt2
NH_ORACLE_HOME - /export/system1/oracle92
```

When specifying the software locations in your LCF, keep in mind the following:

- The settings for the NH_HOME and NH_ORACLE_HOME environment variables in the LCF must match the settings of these variables on the eHealth system. If you have already installed eHealth, do not try to override these settings by using a different value in the LCF.
- You do not have to specify the size of each software product location. If you do, the installation program uses those values to calculate the disk space requirements.

Specify the Database File Layout

In addition to specifying the configuration variables and specifying the software locations, you can also specify the database file layout.

You must include the following object types:

- Each eHealth tablespace (at least once)
- Three CONTROL repositories (for the Oracle control files)
- The ArchiveLogsDir repository (for the archive logs)
- Eight repositories for the database redo log file

Into each object (tablespace or directory), you can place any number of datafiles. To provide this information in the LCF, you must use the following syntax for each line (as defined in the following table):

```
objectType size pathname
```
For an example, refer to the sample LCFs provided in the next section, “Database over Several Disks (UNIX).”

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>objectType</td>
<td>Name of the object (tablespace or directory) into which eHealth should place the datafile. The following are valid values:</td>
</tr>
<tr>
<td></td>
<td>SYSTEM</td>
</tr>
<tr>
<td></td>
<td>NH_ROLLBACK</td>
</tr>
<tr>
<td></td>
<td>NH_TEMP</td>
</tr>
<tr>
<td></td>
<td>NH_USERS</td>
</tr>
<tr>
<td></td>
<td>NH_INDEX</td>
</tr>
<tr>
<td></td>
<td>NH_DATA01</td>
</tr>
<tr>
<td></td>
<td>NH_DATA02</td>
</tr>
<tr>
<td></td>
<td>CONTROL</td>
</tr>
<tr>
<td></td>
<td>ArchiveLogsDir</td>
</tr>
<tr>
<td></td>
<td>REDO1A</td>
</tr>
<tr>
<td></td>
<td>REDO1B</td>
</tr>
<tr>
<td></td>
<td>REDO2A</td>
</tr>
<tr>
<td></td>
<td>REDO2B</td>
</tr>
<tr>
<td></td>
<td>REDO3A</td>
</tr>
<tr>
<td></td>
<td>REDO3B</td>
</tr>
<tr>
<td></td>
<td>REDO4A</td>
</tr>
<tr>
<td></td>
<td>REDO4B</td>
</tr>
</tbody>
</table>

| size | Specifies the size of the datafile in kilobytes, megabytes, or gigabytes. For example: 250 M. If you specify a dash (-) for the size of the directory, eHealth automatically calculates the size. |

| pathname | Specifies the location of the datafile on the local disk partition. |

When specifying a database file layout, follow these guidelines:

- **Specify three (3) Oracle control files in the LCF and assign a unique name to each one.** The pathnames to the control files are stored in the init.ora file. All other pathnames (to database files) are stored inside those control files.

- **Do not specify a size for the control files.** Instead, use a dash (-) to specify the size. In the event of a physical disk failure, Oracle uses these redundant control files to make recovery easier.

**Database over Several Disks (UNIX)**

*Figure 5* is an LCF for an eHealth database on a UNIX system named “bluesky.” As noted in the comment section at the top of the file, it is configured with eight 17 GB partitions and two 33 GB partitions:

```
# UNIX PARTITION     | SIZE | MOUNT-POINT       | eHealth USE
# --------------------+------|-------------------+--------------
# /dev/dsk/c0t1d0s2  | 16.6G| /export/bluesky02 | INDEX        
# /dev/dsk/c0t2d0s2  | 16.6G| /export/bluesky03 | DATA         
```
The eHealth system on bluesky polls 50,000 elements and keeps three days of raw data. It requires 47 GB of space, and the layout will use some space on all disks to minimize disk contention.

# - - - - - - - - - - - - - - - - - - - - - - - - -
# Configuration Variables:
# - - - - - - - - - - - - - - - - - - - - - - - - -
CfgHostname = bluesky
CfgDbModelSize = xlarge
CfgSID = eHealth
CfgRedoLogSize = 156M
CfgNH_USER = nhuser
# - - - - - - - - - - - - - - - - - - - - - - - - -
# Software Locations:
# - - - - - - - - - - - - - - - - - - - - - - - - -
NH_ORACLE_HOME = /export/bluesky01/oracle92
NH_HOME = /export/bluesky01/eHealth
# - - - - - - - - - - - - - - - - - - - - - - - - -
# Database File Layout:
# - - - - - - - - - - - - - - - - - - - - - - - - -
# Put control files on any three distinct disks:
CONTROL = /export/bluesky02/oradata/{SID}/CONTROL01.ctl
CONTROL = /export/bluesky03/oradata/{SID}/CONTROL02.ctl
CONTROL = /export/bluesky04/oradata/{SID}/CONTROL03.ctl
# Give archive logs their own disk:
ArchiveLogsDir = /export/bluesky07/oradata/{SID}/ArchiveLogs
# Give REDO logs their own 4 disks:
REDO1A = /export/bluesky08/oradata/{SID}/REDO1A.log
REDO2A = /export/bluesky10/oradata/{SID}/REDO2A.log
REDO3A = /export/bluesky08/oradata/{SID}/REDO3A.log
REDO4A = /export/bluesky10/oradata/{SID}/REDO4A.log
REDO1B = /export/bluesky09/oradata/{SID}/REDO1B.log
REDO2B = /export/bluesky11/oradata/{SID}/REDO2B.log
REDO3B = /export/bluesky09/oradata/{SID}/REDO3B.log
REDO4B = /export/bluesky11/oradata/{SID}/REDO4B.log
# Give index its own disk:
NH_INDEX = /export/bluesky02/oradata/{SID}/NH_INDEX01.dbf
# Spread all data across three disks:
NH_USERS = /export/bluesky03/oradata/{SID}/NH_USERS01.dbf
NH_USERS = /export/bluesky04/oradata/{SID}/NH_USERS02.dbf
NH_USERS = /export/bluesky05/oradata/{SID}/NH_USERS03.dbf
NH_DATA01 = /export/bluesky05/oradata/{SID}/NH_DATA01a.dbf
NH_DATA01 = /export/bluesky04/oradata/{SID}/NH_DATA01b.dbf
NH_DATA01 = /export/bluesky03/oradata/{SID}/NH_DATA01c.dbf
NH_DATA02 = /export/bluesky05/oradata/{SID}/NH_DATA02a.dbf
NH_DATA02 = /export/bluesky04/oradata/{SID}/NH_DATA02b.dbf
NH_DATA02 = /export/bluesky03/oradata/{SID}/NH_DATA02c.dbf
# Put TEMP, ROLLBACK, and SYSTEM together:
NH_TEMP = /export/bluesky06/oradata/{SID}/NH_TEMP01.dbf
NH_ROLLBACK = /export/bluesky06/oradata/{SID}/NH_ROLLBACK01.dbf
SYSTEM = /export/bluesky06/oradata/{SID}/SYSTEM01.dbf

Figure 5 LCF for Database over Several Disks (UNIX)
Use an LCF during Installation to Size Your Database

**Database on a RAID (UNIX)**

*Figure 6* is an LCF for an eHealth database on a UNIX system named "boston" that is configured with an NFS-mounted RAID of 200 GB. All files will reside in one directory area.

<table>
<thead>
<tr>
<th>UNIX PARTITION</th>
<th>SIZE</th>
<th>MOUNT-POINT</th>
<th>eHealth USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmgr:/export/vol01</td>
<td>199.2G</td>
<td>/export/vol01</td>
<td>EVERYTHING</td>
</tr>
</tbody>
</table>

*We have purposely configured this LCF to keep the size of each datafile under 8G.*

```c
(c) Copyright 2007, CA, Inc.
```

**Figure 6** LCF for Database on a RAID (UNIX)
Database over Several Disks (Windows)

Figure 7 is an LCF for an eHealth database on a Windows system named “wintel” that has fifteen local 20 GB ISDN drives. The eHealth system polls 50,000 elements and saves three days of raw poll data. This requires 47 GB of space, and the layout uses some space on all disks to minimize disk contention.

```
# Configuration Variables:
CfgHostname = wintel
CfgDbModelSize = xlarge
CfgSID = eHealth
CfgRedoLogSize = 156M
CfgNH_USER = nhuser

# Software Locations:
NH_ORACLE_HOME = c:\oracle92
NH_HOME = c:\eHealth

# Database File Layout:

# Put control files on any three distinct disks:
CONTROL = D:\oradata\{SID}\CONTROL01.ctl
CONTROL = E:\oradata\{SID}\CONTROL02.ctl
CONTROL = F:\oradata\{SID}\CONTROL03.ctl
# Put SYSTEM and TEMP together:
NH_TEMP = 2G D:\oradata\{SID}\NH_TEMP01.dbf
SYSTEM = 300M D:\oradata\{SID}\SYSTEM01.dbf
# Leave ROLLBACK on its own disk:
NH_ROLLBACK = 1G E:\oradata\{SID}\NH_ROLLBACK01.dbf
# Give archive logs their own disks:
ArchiveLogsDir = 9766M F:\oradata\{SID}\ArchiveLogs
# Give REDO logs their own 4 disk:
REDO1A = G:\oradata\{SID}\REDO1A.log
REDO2A = I:\oradata\{SID}\REDO2A.log
REDO3A = G:\oradata\{SID}\REDO3A.log
REDO4A = I:\oradata\{SID}\REDO4A.log
REDO1B = H:\oradata\{SID}\REDO1B.log
REDO2B = J:\oradata\{SID}\REDO2B.log
REDO3B = H:\oradata\{SID}\REDO3B.log
REDO4B = J:\oradata\{SID}\REDO4B.log
# Spread INDEX across three disks:
NH_INDEX = 3G K:\oradata\{SID}\NH_INDEX01.dbf
NH_INDEX = 3G L:\oradata\{SID}\NH_INDEX02.dbf
NH_INDEX = 3G M:\oradata\{SID}\NH_INDEX03.dbf
# Spread all data across five disks:
NH_USERS = 100M N:\oradata\{SID}\NH_USERS01.dbf
NH_USERS = 100M O:\oradata\{SID}\NH_USERS02.dbf
NH_USERS = 100M P:\oradata\{SID}\NH_USERS04.dbf
NH_USERS = 100M Q:\oradata\{SID}\NH_USERS05.dbf
NH_DATA01 = 3G R:\oradata\{SID}\NH_DATA01a.dbf
NH_DATA01 = 3G Q:\oradata\{SID}\NH_DATA01b.dbf
NH_DATA01 = 3G P:\oradata\{SID}\NH_DATA01c.dbf
NH_DATA01 = 3G O:\oradata\{SID}\NH_DATA01d.dbf
NH_DATA01 = 3G N:\oradata\{SID}\NH_DATA01e.dbf
NH_DATA02 = 2G P:\oradata\{SID}\NH_DATA02a.dbf
NH_DATA02 = 2G Q:\oradata\{SID}\NH_DATA02b.dbf
NH_DATA02 = 2G R:\oradata\{SID}\NH_DATA02c.dbf
NH_DATA02 = 2G N:\oradata\{SID}\NH_DATA02d.dbf
NH_DATA02 = 2G O:\oradata\{SID}\NH_DATA02e.dbf
```

Figure 7 LCF for Database over Several Disks (Windows)
A
accounts  
  listing • 141  
  managing • 141
adding, datafile • 151
administration concepts  
  cluster • 12  
  elements • 61
advanced logging for troubleshooting • 271
AdvantEDGE View  
  application queries • 190
agent type, changing • 76
agents  
  NSM • 112  
  SystemEDGE • 112
AIM, Oracle • 112
all conversations data, rolling up • 121
alternate latency  
  configuring • 218  
  disabling • 220  
  modifying elements • 218  
  partners • 217  
  creating • 220  
  deleting • 220
analyzed data • 116
application  
  monitoring effects on systems • 175  
  reports  
    At-a-Glance • 194  
    MyHealth • 195  
    overview • 193  
    Top N • 195  
    Trend • 194
Application Insight  
  collecting data • 188  
  license • 187
application service  
  discovering elements • 190  
  elements • 191  
  process sets • 190, 191
archive logs  
  deleting • 119  
  description • 110  
  with incremental save • 129
archiving, database saves • 127
ASCII saves • 124
At-a-Glance reports  
  applications • 194  
  systems • 184
B
backups  
  archiving • 127  
  best practices • 127  
  cross-platform • 124, 138  
  disk locations • 128  
  disk space requirements • 125  
  full (incremental) • 123  
  full (universal) • 124  
  how saves work • 124  
  incremental • 123  
  monitoring disk space • 131  
  performing immediate • 126  
  platform-dependent • 123  
  platform-independent • 124, 138  
  scheduling  
    incremental • 128  
    standard • 130  
  standard • 123  
  third-party tools • 111, 123  
  tips • 126  
  universal • 124, 138
baseline argument • 244
baselineType argument • 244
best practices  
  database backups • 127  
  database recovery • 132  
  database saves • 126  
  database security • 140
C
changing
database size • 142, 143
user passwords • 140, 142
user passwords when Report Center is installed • 142
chartType argument • 245
checking disk space
before loading database • 132
cleanup nodes, scheduled job • 121
collecting data
application • 188
system • 174
commands
nhChangeDbModelSize • 143
nhConfigDbNet • 144
nhCreateDb • 135
nhDestroyDb • 135
nhExpire • 150
nhLoadDb • 124, 136
nhLoadDb -fullRecovery • 133
nhLoadDb -pointInTimeRecovery • 134
nhLoadDb -showRecoveryTimeRange • 134
nhManageUsers • 141, 142
nhSaveDb • 127
nhSaveDbConfig -delete • 130
nhSaveDbConfig -list • 130
nhSchedule • 118, 131
nhServer • 18, 19, 133, 135, 137, 140, 143, 152
nhStopDb • 139
community string, changing • 74
community string, specifying • 53
component
discover key format • 200
connection, troubleshooting database • 145
collection poll rate • 64
collection poll rate, changing • 64
conversations
all • 121
data rollups • 117
disk space usage • 116
rollup job • 121
top • 121
core files, deleting • 149
creating
groups
applications • 192
process sets • 177
CRN database user, changing password • 142
cross-platform
moving database • 138
saves • 124
D
data
analyzed • 116
conversations • 116
preventing loss • 127
rollup • 115
database
archive logs • 110
archiving backups • 127
backups
overview • 123
See Also backups.
checking disk space
available • 145, 148
before loading • 132
connection problems • 145
deleting archive logs • 119
displaying status • 145
full recovery (incremental) • 133
full recovery (standard) • 135
lack of space problems • 148, 151
listing user accounts • 141
loading
overview • 132
See Also loading database.
log files • 114
logs, archive • 110
logs, redo • 110
maintenance job • 120
managing
overview • 109
users • 140
moving
cross-platform • 138
Distributed eHealth • 139
same platform • 136
overview • 109, 110
partial recovery • 136
password file • 142
passwords • 140, 142
performance upgrades • 111
point-in-time recovery • 134
preventing data loss • 127
reclaiming disk space • 149
recovery
  overview • 132
  See Also recovering database.
redo logs • 110
rollup schedule • 115
saving full • 126
scheduling backups • 130
security • 140
size, changing • 142, 143
statistics rollup schedule • 115
status • 113, 145, 148
stopping • 139
third party backup software • 123
understanding • 110
datafile
  adding • 151
  description • 110
  moving • 151
dayOptions argument • 245
default scheduled jobs
  deleting • 167
  description • 161
defining process sets • 176
Delete Old Reports scheduled job • 150
deleting
  archive logs • 119
  core files • 149
  incremental save job • 129
  old reports • 120
  process from process set definition • 179
  process set definition • 179
  temporary files • 150
  temporary tables • 120
devices
  verifying match • 198
discover
  changing resources • 67
  comparing
    unique keys • 199
  element types
    system • 208
  filtering elements • 48
  identifying devices in network • 38
impact of resource changes • 67
IP address file, using • 50
jobs, adding • 58
keys, creating • 200
log
  interactive discover • 43
  reporting discover results • 198
planning for
  frequent network changes • 67
technology
  Application • 208
  LAN/WAN • 205
  Modem Pool • 209
  Probes • 207
  QoS • 210
  Remote Access Server • 209
  Router • 206
  System • 208
upgrading network devices • 59
verifying device match • 198
Discover Policy parameters
  DNS Lookup by ifIpAddress • 213
  Naming - Truncate by Regular Expressions • 213
  Naming - Use DNS • 212
  Ports - All • 39
  Ports - Application • 39
  Ports - Response • 39
  Ports - System • 39
  Timeout • 52
discover process
  identifying resources • 38
  starting • 42
discovering
  application elements • 190
  process sets • 176
  system elements • 174
disk locations for backups • 128
disk space
  available in database • 145
  checking before database load • 132
  monitoring for backups • 131
  reclaiming • 149
  required for saves • 125
  solving problems • 148
Distributed eHealth
  moving database • 139
  scheduled jobs • 122
divBy argument • 245
DNS Lookup by ifIpAddress • 213
duplicate elements
  same attributes • 45
  same names, different attributes • 44

E
eHealth
  AIMS, monitoring the Oracle database • 112
  application reports
    At-a-Glance • 194
    MyHealth • 195
    Top N • 195
    Trend • 194
database. See database.
  elements • 61
  maintenance
    upgrading • 14
  polling • 64
  running reports
    applications • 193
    systems • 183
  server
    starting • 133, 134, 135, 137
    stopping • 18, 19, 133, 134, 135, 137, 140, 143, 152
  Sizing Wizard. See Sizing Wizard.
  system reports
    At-a-Glance • 184
    MyHealth • 185
    Top N • 184
    Trend • 184
    What-If Capacity Trend • 184
  systems
    remote polling • 12
    standalone • 12
    Traffic Accountant • 13
    using with SystemEDGE • 175
eHealth AIMS
  applications monitored • 189
  collecting application data • 188
  element configuration
    agent type, changing • 76
    modifying • 78
      agent type • 76
    speed, changing • 77
    viewing • 61
  element types, discovering
    enhanced router/switch • 206
    LAN/WAN • 205
  Remote Access Servers • 209
    router LAN/WAN • 206
    router/switch • 206
    switch Lite switches • 207
  system • 208
  Traffic Accountant • 207
elements • 61
  changing
    agent type • 76
    community strings • 74
    description information • 77
    retries rate • 75
    speed • 77
    timeout rate • 75
database growth • 114
duplicates • 45
  exporting a simple name list • 63
  filtering discoveries • 48
  properties, updating • 78
  retiring • 85
  turning off polling • 68
type of network interface • 205
elements, discovering
  application • 190
  system • 174
  enableScalingPercentAxis argument • 245
environment variables
  NH_CISCO_PING_DISABLED • 220
  NH_POLL_PING_DISABLED • 74
  NH_POLL_PING_PKTSIZE • 73
  NH_SNMP_DEVICE_RETRIES • 70
  NH_SNMP_DEVICE_TIMEOUTS • 70
  NH_SNMP_RETRIES • 75
  NH_SNMP_TIMEOUT • 71, 75
errors, scanning log files • 114
execute=Generate+Report argument • 245

Files
  adding datafiles • 151
  core, deleting • 149
  database password • 142
  log • 114
  moving datafiles • 151
  saved during backup • 125
  temporary, deleting • 150
  filtering, discovered elements • 48
Frame Relay elements, discovering • 205
Frame Relay, adding PVC elements • 85, 87
fromDate argument • 245
fromTime argument • 245
full recovery
  from incremental save • 133
full recovery, from standard save • 135
full saves
  incremental • 123
  performing immediate • 126
  scheduling • 128, 130
  universal • 124
func argument • 245

G

goal argument • 246
goalLineLabel argument • 246
goalLineValue argument • 246
granularity argument • 246
groups
  controlling access to • 90
  creating • 91, 93
  editing • 96
groups, creating
  applications • 192
growth
  analyzed data • 116
  data • 115
  factors that drive • 114
  number of elements • 114

H

Health reports
  overview • 185
history
  sampling • 172

I

identifying resources • 38
ifDescr variable
  using unique • 59
incremental saves
  deleting scheduled job • 129
  example • 129
  full recovery from • 133
  level 0 • 123
  level 1 • 123
  overview • 123
  partial recovery from • 136
  point-in-time recovery from • 134
  scheduling • 128
IP addresses
  discover using file • 50
  discovering elements • 56

J

job scheduler, using • 165
jobs
  cleanup nodes • 121
  conversations rollup • 121
  database maintenance • 120
  delete archive logs • 119
  delete old reports • 120
  delete temporary tables • 120
  Distributed eHealth • 122
  statistics rollup • 117

L

LAN/WAN elements, discovering • 205
latency partners • 217
level 0 saves
  overview • 123
level 1 saves
  overview • 123
Live Exceptions
  history • 119
  modifying scheduled jobs • 119
Live Health
  Fault Manager • 186
  using with SystemEDGE • 186
loading database
  cross-platform • 138
  incremental, full • 133
  incremental, point-in-time • 134
  overview • 132
  partial • 136
  standard, full • 135
localized argument • 246
logging troubleshooting information • 271
logs
  archive • 110, 129
M

maintenance, database scheduled job • 120
managing jobs
  enabling and disabling • 164
managing users • 141, 142
mapped drives • 128
maxYValuePercentAxis argument • 246
mediumType argument • 247, 248, 249, 250
model size, changing • 142
modem pool
  changing default • 210
  defining in agent • 210
  discovering • 209
  types of elements • 210
modem pool element, creating • 86
monitoring
  database health • 112
  disk space for backups • 131
  Oracle processes • 112
moving database
  cross-platform • 138
  Distributed eHealth • 139
  same platform type • 136
moving, datafiles • 151
MyHealth reports
  applications • 195
  systems • 185

N

nameFilter argument • 250
Naming - Truncate by Regular Expressions • 213
Naming - Use DNS • 212
network
  changes, understanding • 38
  identifying devices • 38
  obtaining IP addresses of devices • 38
  resolvable changes • 45
network configuration, modifying Oracle • 144
NFS-mounted disks • 128
NH_POLL_PING_DISABLED • 73
NH_POLL_PING_PKT_SIZE • 73
NH_SNMP_DEVICE_RETRIES • 70
NH_SNMP_DEVICE_TIMEOUTS • 70
NH_SNMP_RETRIES • 75
NH_SNMP_TIMEOUT • 71, 75
nhChangeDbModelSize command • 143
nhConfigDbNet command • 144
nhCreateDb command • 135
nhDestroyDb command • 135
nhExpire command • 150
nhListElements command • 63
nhLoadDb command • 124, 133, 134, 136
nhManageUsers command • 141, 142
nhSaveDb command • 127
nhSaveDbConfig command • 130
nhSchedule command • 118, 131
nhServer command • 18, 19, 133, 135, 137, 140, 143, 152
nhStopDb command • 139
nodes, cleanup job • 121
Normal polling rate, defined • 64
NSM agent • 112

O

OneClickEH
eHealth history
  database alerts • 158
Oracle
  AIM • 112
  database installed with eHealth • 109
  modifying network configuration • 144
  patches • 111
  Recovery Manager • 122
  space problems • 151
Oracle. See also database
overview
  database • 109, 110
  datafiles • 110
  tablespaces • 110
Index

P

parent name, modifying • 77
partial recovery from incremental save • 136
partialDayStart argument • 250
partialDayStop argument • 250
partialWeek argument • 250

passwords
  changing • 140
  changing when Report Center is installed • 142
  password file creation, database • 142
  specifying for database users • 142

patches, Oracle • 111

performance upgrades, database • 111
platform, moving database across • 138

point-in-time recovery, incremental save • 134
polled elements, database growth • 114
poller configuration
  modifying
    community string • 74
polling
  interval, setting • 64
  rates
    changing for all elements • 64
    controlling for individual elements • 65

Ports - All, Discover Policy parameters • 39
Ports - Application, Discover Policy parameters • 39
Ports - Response, Discover Policy parameters • 39
Ports - System, Discover Policy parameters • 39
problems
  database access • 145
  database load • 133
  disk space • 148
process elements • 177
process sets
  creating for an application • 177
  defining • 54, 176
  deleting processes • 179
  discover rules, using • 176
  discovering • 176, 208
  example • 179
  licensing • 208
  reporting on individual elements • 177

protocol argument • 251
protocol2 argument • 251
PVC elements, adding • 87

Q

QoS elements, discovering • 210

R

range, time for recovery • 134
RAS
  discovering • 209
  managing
    as modem pools • 209
    as physical device • 209
  types of elements • 209
reclaiming disk space • 149
recovery database
  incremental, full • 133
  overview • 132
  partial • 136
  point-in-time • 134
  standard, full • 135
  tips • 132
recovery time range, point-in-time recovery • 134
redo logs • 110
reducing database size • 143
remote access server. See RAS. • 209
remote polling • 12
report argument • 252
reports
  At-a-Glance
    applications • 194
    system • 184
  cleaning up old files • 150
  Delete Old Reports scheduled job • 120
  deleting • 120
  Health • 185
  MyHealth
    applications • 195
    systems • 185
  removing old report files • 150
  running
    applications • 193
    systems • 183
  Service Level • 185
Top N
  applications • 195
  systems • 184
Trend
  applications • 194
  systems • 184
What-If Capacity Trend • 184
reportType argument • 252
resizing, database • 143
response elements, discovering • 210
restoring database. See recovering database.
retiring elements • 85
retries rate, changing • 75
rollup
  about conversations • 115
  about statistics • 115
  conversations • 117
  conversations job • 121
data • 115
default schedule for statistics • 117
  modifying • 117
  schedule • 115
router
  discovering elements • 206
  reporting
    enhanced • 206
    standard • 206
rules, using in discover • 49
S
saves
  archiving • 127
  ASCII • 124
  best practices • 127
  disk locations • 128
  how saves work • 124
  incremental • 123
  performing full (standard) • 126
  performing immediate • 126
  scheduling incremental • 128
  scheduling standard • 130
  universal • 124
scheduled discover job • 57
scheduled jobs
  cleanup nodes • 121
  conversations rollup • 121
database maintenance • 120
delete archive logs • 119
delete old reports • 120
delete temporary tables • 120
Distributed eHealth • 122
enabling and disabling • 164
  modifying • 118
scheduling
  incremental saves • 128
  standard saves • 130
  statistics database rollups • 117
scheduling discovery
  application elements • 191
  system elements • 174
secondary consoles
  administration tasks • 221
  running with Telnet • 227
  running with Terminal Services • 226
  setting options • 223
  summary of restrictions • 222
  using Poller Configuration dialog • 223
security, database • 140
self monitoring • 172
Service Level reports • 185
serviceProfile argument • 252
showGoalLine argument • 252
size
  changing database • 142
  reducing database • 143
Sizing Wizard
  changing database size • 143
  description • 111
  location • 111
  using • 111
sortOrder argument • 252
space
  checking before loading database • 132
  monitoring for backups • 131
  required for saves • 125
  solving problems • 148
specifying timeout for SNMPv3 discovery process • 52
speed, changing for elements • 77
standard save
  full recovery from • 135
  performing immediate • 126
scheduling • 130
statistics rollup
  changing the rollup schedule • 118
  overview • 117
status, viewing database • 145
stopping, database • 139
subject argument • 253
subjectType argument • 253
SWIZ. See Sizing Wizard.
syName variable
  using unique values • 59
system
  definition of elements • 208
  identifying elements • 173
  process
    creating elements • 174
    definition file • 176
    deleting • 179
  process set definition
    deleting • 179
    modifying • 179
  process sets
    defining • 176
    discovering • 176
    example • 179
reports
  At-a-Glance • 184
  Health • 185
  MyHealth • 185
  overview • 182
  Service Level • 185
  Top N • 184
  Trend • 184
  What-If Capacity Trend • 184
system description, modifying • 77
SystemEDGE • 112
SystemEDGE agent
  self-monitoring features • 172
T
  looking through reports • 194
  tables, deleting temporary • 120
  tablespaces
    description • 110
    full • 151
templateName argument • 253
temporary files, deleting • 150
temporary tables, deleting • 120
time range, point-in-time recovery • 134
timeOptions argument • 253
  Timeout • 52
timeout rate, changing • 75
timeout, specifying for SNMPv3 discover process • 52
timeRangeType argument • 254
timezone argument • 254
toDate argument • 254
toDateDayOf argument • 254
  toDateMonthOf argument • 254
top conversations, rolling up • 121
Top N reports
  applications • 195
  systems • 184
topN argument • 255
topNF1trDir argument • 255
topNF1trShow argument • 255
topNF1trVal argument • 255
topNValue argument • 255
topNvar argument • 255
toTime argument • 255
Traffic Accountant • 13
Traffic Accountant elements • 207
traps, handling
  Fault Manager • 186
Trend reports
  applications • 194
  systems • 184
troubleshooting
  database connection • 145
  disk space problems • 148
  missed polls • 291
  reducing space demand • 150
U
  Unicenter NSM agent • 112
  universal saves • 124
  usePlannedDowntime argument • 256
users
  database accounts • 140
  managing passwords • 140
userVars argument • 256
using the Sizing Wizard • 111

W
  webReportSubtitle argument • 257
  webReportTitle argument • 256
  webServerUrl argument • 257
  What-If Capacity Trend reports • 184

V
  variable argument • 256